

VÅRA ÖVERVÄGANDEN

7 Övergripande frågor och principer

7.1 Behovet av datorstöd

Inom den militära underrättelse- och säkerhetstjänsten utgör användningen av datorer sedan många år ett naturligt och omfattande inslag i arbetet. För Försvarets radioanstalts underrättelseverksamhet är hantering av uppgifter med hjälp av datorer den helt dominerande arbetsmetoden. I båda verksamheterna pågår en ständig teknisk utveckling av datorsystemen och lagstiftning som reglerar användningen av datorstöd måste därför vara teknikneutral och flexibel, för att inte hindra framtida effektivisering av verksamheterna.

Det är näst intill omöjligt för lagstiftaren att hålla jämn takt med den informationstekniska utvecklingen. För att inte hamna i en situation där den tekniska utvecklingen styr den rättsliga regleringen, eller där den rättsliga regleringen onödigt hämmar effektiviseringen, är det enligt vår mening nödvändigt med en lagstiftning som enbart tar sikte på principiellt viktiga frågor. Detaljfrågor måste regleras i annan ordning än i lag. Lagstiftningen skall med andra ord på ett övergripande plan styra hur personuppgifter får behandlas med hjälp av dator teknik samtidigt som den rättsliga regleringen inte får tillåtas förhindra eller försvåra en välkommen effektivisering, om det inte är nödvändigt av integritetsskäl.

7.2 Skyddet för den personliga integriteten

De grundläggande bestämmelserna till skydd för den personliga integriteten finns i regeringsformen. Redan i 1 kap. 2 § slås fast att det allmänna skall värna om den enskildes privatliv. Denna intention kommer till uttryck i stora delar av den lagstiftning som reglerar det allmännas handlande gentemot enskilda och även

enskildas handlande gentemot varandra. Som exempel på sådan lagstiftning kan nämnas sekretesslagen (1980:100). Av stor betydelse är även rätten för enskilda att enligt 2 kap. tryckfrihetsförordningen ta del av allmänna handlingar (handlingsoffentlighet). Härigenom garanteras enskilda insyn i och kontroll av den offentliga förvaltningen, vilket kan vara positivt från integritetssynpunkt. Offentligheten kan emellertid även innebära nackdelar från integritetssynpunkt, eftersom enskilda tvingas acceptera att uppgifter om dem kan vara åtkomliga för andra personer.

I 2 kap. 3 § andra stycket regeringsformen finns en särskild bestämmelse som avser integritetsskyddet vid automatiserad behandling av personuppgifter. Där sägs att varje medborgare, i den utsträckning som närmare anges i lag, skall skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatisk databehandling. Den författning som i dag har som syfte att i första hand uppfylla regeringsformens intentioner i fråga om integritetsskydd i datoriserad verksamhet är personuppgiftslagen (1998:204). Härutöver finns särskilda registerförfattningar som reglerar en stor del av den offentliga verksamheten. Integritetsskyddande bestämmelser om utlämnande av personuppgifter finns även i sekretesslagen.

Det är inte möjligt att definiera exakt vad som avses med personlig integritet. Inte minst är det svårt på grund av att uppfattningen om vad som är en rent personlig sfär varierar mellan olika personer. Dessutom förändras inställningen till integritet över tiden. Det kan också konstateras att varken svensk lagstiftning eller doktrin innehåller någon enhetlig definition av begreppet. När det gäller uppgifter som är personliga kan det också ha betydelse i vilket sammanhang de används om den enskilde uppfattar det som att hans integritet har kränkts eller inte. Av allt att döma finns det emellertid enighet om att vissa faktorer är särskilt viktiga att ta hänsyn till när det gäller att bedöma integritetskänsligheten vid automatiserad behandling av personuppgifter. Det gäller arten av personuppgifter som samlas in och registreras, varför detta görs, hur och av vem uppgifterna används samt mängden av uppgifter som samlas på ett och samma ställe eller som på något annat sätt är tillgängliga för bearbetningar och sammanställningar. Samtidigt bör beaktas att rätten till personlig integritet inte är absolut utan från tid till annan föremål för inskränkningar. En väl fungerande samhällsorganisation kommer alltid att medföra intrång i enskildas personliga integritet. Avgörande blir i detta sammanhang vad som

kan tolereras och vad som utgör ett *otillbörligt* intrång i den personliga integriteten.

Enligt vår mening kan stora informationsmängder, som är samlade så att uppgifter är enkelt sökbara på elektronisk väg och som används vid myndighetsverksamhet, medföra en påtaglig risk för att enskilda personer utsätts för icke acceptabla intrång i den personliga sfären. Den militära underrättelse- och säkerhetstjänstens samt Försvarets radioanstalts användning av datorer kan alltså i och för sig utgöra ett hot mot den personliga integriteten. Detta måste beaktas vid utformningen av lagstiftningen inom området. Vid bedömningen av hur integritetsintressena skall tas till vara måste emellertid hänsyn också tas till de speciella verksamheter som myndigheterna bedriver. Det är av naturliga skäl inte önskvärt att genom begränsande regler för behandlingen av personuppgifter frånta Försvarmakten och Försvarets radioanstalt möjligheten att bedriva en till skydd för Sveriges intressen och säkerhet effektiv underrättelseverksamhet och säkerhetstjänst. Det måste också beaktas att verksamheterna av naturliga skäl i stora delar är hemliga och att de personuppgifter som behandlas därför i mycket stor omfattning omgärdas av sekretess. Dessutom ställs det även utan särskild integritetsskyddande lagstiftning mycket höga krav på bl.a. datasäkerhet och spridning av uppgifter till utomstående.

Försvarsunderrättelseverksamhet och säkerhetstjänst utgör grundläggande och viktiga samhällsfunktioner för Sveriges oberoende och den nationella säkerheten. Dessa verksamheter måste därför bedrivas på ett effektivt och ändamålsenligt sätt vilket bl.a. förutsätter ett rationellt datorstöd för behandling av personuppgifter. Detta hindrar emellertid inte att nödvändig respekt visas för enskildas personliga integritet vid myndigheternas behandling av personuppgifter. En författningsreglering måste beakta båda dessa, i bland motstående, intressen.

Mot bakgrund av de aktuella verksamheternas art är det enligt vår uppfattning två omständigheter som framstår som särskilt avgörande för författningsregleringen av myndigheternas behandling av personuppgifter. 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.

Som i all annan offentlig verksamhet, eller i andra sammanhang där en stor mängd personuppgifter behandlas, är det ur integritets-synvinkel av grundläggande betydelse att behandlingen av personuppgifter endast sker för särskilt fastställda ändamål. Med tydliga

ändamål för vilka behandling av personuppgifter får ske kan den enskilde på ett enkelt sätt få en tydlig bild av om uppgifter om honom eller henne behandlas eller inte, och om så sker i vilken omfattning detta kan komma att medföra ett otillbörligt intrång i hans eller hennes personliga integritet. Om risk för sådant intrång föreligger kan den registrerade med hjälp av de särskilda rättigheter som tillkommer enskilda enligt personuppgiftslagen eller motsvarande lagstiftning, om information och rättelse m.m., vidta åtgärder för att få detta hot undanröjt.

Med hänsyn till Försvarmaktens och Försvarets radioanstalts arbetsuppgifter i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten ligger det i sakens natur att verksamheten till stor del måste vara hemlig. Många uppgifter är känsliga såväl med hänsyn till Sveriges förhållande till främmande makt som till skydd för rikets säkerhet. Det är också viktigt att skydda uppgiftslämnare och arbetsmetoder. Det skulle t.ex. bli betydligt svårare för den militära underrättelse- och säkerhetstjänsten att få den information från utländska underrättelse- eller säkerhetstjänster eller andra källor som myndigheten behöver, om inte verksamheten var omgärdad av sekretess.

De krav på säkerhet och sekretess som gäller för uppgifter i de aktuella verksamheterna ger särskilda förutsättningar när det gäller skyddet för den personliga integriteten. Med säkerhet avses i första hand en teknisk informationssäkerhet, till skydd för intrång i de datorsystem som används, i syfte att förhindra att obehöriga får tillgång till de uppgifter som behandlas. Med sekretess avses att uppgifterna är hemliga och vid straffansvar inte får lämnas ut med mindre än att reglerna i sekretesslagen medger det. Den säkerhet och sekretess som omgärdar försvarsunderrättelseverksamhet och militär säkerhetstjänst medför således att det i jämförelse med annan verksamhet är mindre risk för att personuppgifter sprids till utomstående. Härmed är det i motsvarande mån en mindre risk för att uppgifterna skall behandlas för andra ändamål än syftet med den ursprungliga behandlingen. Redan de förutsättningar under vilka verksamheterna bedrivs utgör således ett *skydd mot* otillbörligt intrång i den personliga integriteten.

Att verksamheten är sluten och att det till följd härav är svårt för de registrerade att få insyn i den behandling av personuppgifter som sker kan emellertid även medföra *risk för* otillbörligt intrång i den personliga integriteten. Utan insyn i och kunskap om den verksamhet som bedrivs kan det vidare lätt födas uppfattningar om att det begås någon form av oegentligheter från myndigheternas

sida. Med hänsyn till verksamheternas art måste emellertid den mycket omfattande sekretessen gälla. Härifrån kan inte göras undantag för att eventuellt stärka skyddet av den personliga integriteten. I den utsträckning enskildas möjlighet till information m.m. inte utgör ett fullgott skydd för den personliga integriteten måste denna värnas på något annat sätt. Enligt vår mening kan detta, med iakttagande av den sekretess och säkerhet i övrigt som måste omgärda verksamheterna, bäst ske genom att ett från de aktuella verksamheterna fristående och oberoende organ ges i uppdrag att särskilt granska behandlingen av personuppgifter. En sådan granskning ger de registrerade en indirekt insyn i behandlingen av personuppgifter till skydd för den personliga integriteten.

Det vi anser är viktigast i samband med en reglering av användningen av datorer och dataregister inom den militära underrättelse- och säkerhetstjänstens samt Försvarets radioanstalts verksamheter är således för vilka ändamål uppgifter från olika källor får behandlas. Även andra faktorer har emellertid betydelse, t.ex. behandling av känsliga personuppgifter och spridningen av information till utomstående. I fråga om vilka som får ta del av uppgifter intar omfattningen av myndigheters och andras direktåtkomst till elektroniskt lagrad information en särställning.

Vi kommer att behandla de olika integritetsaspekterna efterhand som vi redovisar vår inställning i de olika sakfrågorna, t.ex. gällande direktåtkomst. Redan här bör emellertid slås fast att vi anser det viktigt att en författningsreglering om användning av datorer inom de båda myndigheterna utformas på ett sådant sätt att hänsyn i tillräcklig omfattning tas till integritetsskyddet för enskilda.

Sammanfattningsvis är det vår uppfattning att de aktuella verksamheterna utgör så grundläggande och viktiga samhällsfunktioner att de måste bedrivas på ett ändamålsenligt och effektivt sätt, även om det av vissa kan uppfattas som ett intrång i den personliga integriteten. Behandling av personuppgifter som uteslutande sker enligt de för verksamheten särskilt fastlagda ändamålen utgör – med beaktande av den sekretess och säkerhet i övrigt som gäller i verksamheten – inte i sig någon påtaglig risk för *otillbörligt* intrång i de registrerades personliga integritet. Detta hindrar emellertid inte att vissa användningar, såsom t.ex. behandling av känsliga personuppgifter och andras direktåtkomst till elektroniskt lagrad information måste regleras särskilt. För att motverka den brist på insyn som följer av reglerna om sekretess bör vidare ett fristående och oberoende organ få till särskild uppgift att granska behandlingen av personuppgifter. Sådan granskning skall ske för att

säkerställa att behandlingen av personuppgifter endast sker för de i lag fastställda ändamålen och för att tillförsäkra att otillbörligt intrång i de registrerades personliga integritet inte sker.

7.3 Särskild författningsreglering

Vårt förslag: Behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet skall författningsregleras särskilt. Uppgifter i den interna administrationen skall behandlas enligt personuppgiftslagens bestämmelser.

Allmänna bestämmelser om integritetsskydd inom datorområdet finns, som nämnts tidigare, i personuppgiftslagen. För olika offentliga verksamheter kan dock integritetsproblemen vara av skiftande art. Det går därför inte generellt att lösa alla problem och fullt ut beakta alla frågeställningar genom att vända sig till personuppgiftslagens bestämmelser, utan det behövs ofta särskild författningsreglering. En förutsättning är att sådan reglering inte strider mot EU:s dataskyddsdirektiv när detta är tillämpligt. När det gäller dataskyddsdirektivets tillämplighet bör emellertid i detta sammanhang framhållas vad som anges i direktivets artikel 3.2 första strecksatsen. Enligt denna bestämmelse gäller direktivet inte för sådan behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välbefinnande när behandlingen har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område. I kommissionens förklaring till bestämmelsen anges säkerhetstjänst som exempel på en aktivitet som faller utanför tillämpningsområdet (se SOU 1997:39 s. 120). Med hänsyn härtill omfattas inte Försvarmaktens försvarsunderrättelseverksamhet, den militära säkerhetstjänsten eller Försvarets radioanstalts underrättelseverksamhet av dataskyddsdirektivets bestämmelser. Vår utgångspunkt har naturligtvis ändå varit att våra författningsförslag inte skall strida mot de grundläggande och bindande principerna i dataskyddsdirektivet, även om det skulle vara EG-rättsligt möjligt.

Särskild författningsreglering bör enligt vår uppfattning tillämpas endast om det finns beaktansvärda skäl för det. Vi anser att man generellt kan peka ut de situationer då så normalt är fallet, nämligen

- när en nödvändig behandling över huvud taget inte är tillåten enligt personuppgiftslagen, t.ex. i fråga om behandling av vissa känsliga uppgifter,
- när personuppgiftslagen visserligen reglerar ett visst förhållande, men det finns anledning att avvika från eller precisera den regleringen, t.ex. i fråga om hur länge uppgifter får bevaras,
- när personuppgiftslagens bestämmelser kan ge upphov till tolkningsproblem och det finns anledning att ha tydliga bestämmelser, t.ex. i fråga om vem som är personuppgiftsansvarig,
- när det finns anledning att begränsa möjligheterna till behandling av uppgifter av integritetsskäl, t.ex. i fråga om myndigheters registrering av och åtkomst till stora eller känsliga uppgiftsmängder, samt
- när det finns anledning att vara särskilt tydlig gentemot allmänheten, t.ex. i fråga om vilka uppgifter om enskilda som olika myndigheter registrerar.

Enligt vår uppfattning behövs en särskild författningsreglering av behandlingen av personuppgifter inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet av såväl effektivitets- som integritetsskäl. Bland annat omfattningen av verksamheterna, deras speciella inriktning samt den stora mängden känsliga uppgifter och behandlingar som förekommer, utesluter att personuppgiftslagen skall vara den enda författning som reglerar informationshanteringen.

När det däremot gäller den interna administrativa förvaltningen, exempelvis lokal- och personalfrågor, är situationen en helt annan. Administrationen av sådana frågor påminner mestadels om hanteringen av information hos vilken större arbetsgivare som helst. Internt administrativt arbete vid en myndighet är normalt inte reglerad i registerförfattningar för annan offentlig verksamhet och vi kan inte se annat än att personuppgiftslagens regler är fullt tillräckliga för att hantera behandlingen av personuppgifter i t.ex. löneregister.

7.4 Lag, förordning eller myndighetsföreskrifter

Vårt förslag: De grundläggande principerna för behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet skall regleras i lag. Kompletterande bestämmelser meddelas av regeringen eller den myndighet som regeringen bestämmer.

Vi konstaterar i föregående avsnitt att behandling av personuppgifter hos den militära underrättelse- och säkerhetstjänsten och Försvarets radioanstalt måste författningsregleras särskilt. En viktig fråga är i vilken form en sådan författningsreglering skall ske; genom lag, förordning eller myndighetsföreskrifter. I verksamheterna behandlas mängder av uppgifter om enskilda personer i olika register eller datorsystem. Uppgifterna kan i många fall vara mycket känsliga och det är därför viktigt att de behandlas på ett sådant sätt att vederbörlig hänsyn tas till de registrerades personliga integritet.

Frågor om regleringen av personregister har behandlats av konstitutionsutskottet, som bl.a. påpekat att myndighetsregister med ett stort antal registrerade och ett känsligt innehåll skall regleras särskilt i lag (bet. 1990/91:KU11 s. 11 och 1997/98:KU18 s. 48), en uppfattning som även regeringen har gett uttryck för (se bl.a. prop. 1990/91:60 s. 58 och 1997/98:44 s. 41). Enligt vår uppfattning är den automatiserade behandling av personuppgifter som förekommer i den militära underrättelse- och säkerhetstjänstens samt Försvarets radioanstalts verksamheter utan tvekan av sådan karaktär och omfattning att de grundläggande principerna för behandlingen skall slås fast i lag.

Vad vi anser måste framgå av lag är främst sådana grundläggande bestämmelser som anger för vilka ändamål personuppgifter får behandlas, vem som får ha direktåtkomst och under vilka förutsättningar känsliga personuppgifter får behandlas samt vilka rättigheter enskilda har. I vissa fall bör sådana bestämmelser vara ovillkorliga, medan regeringen i andra fall bör kunna medge undantag. Regeringen bör dessutom kunna meddela vissa kompletterande bestämmelser. Som vi nämner ovan i avsnitt 7.2 måste vid utformningen av lagstiftning om behandling av personuppgifter hänsyn tas till att verksamheterna vid de båda myndigheterna är av

grundläggande betydelse för Sveriges yttre säkerhet och för att stärka samhället vid svåra påfrestningar i fred. Sådan lagstiftning måste därför vara övergripande och utformad på ett sådant sätt att verksamheterna kan bedrivas mest effektivt. På motsvarande sätt framhålls även i förarbetena till lagen (2000:130) om försvarsunderrättelseverksamhet att underrättelseverksamheten är av sådan art att det av naturliga skäl inte är möjligt att i lagform reglera den i detalj, utan att riksdagen endast får ge utgångspunkterna för den närmare reglering av verksamheten som sedan kan regleras i detalj med stöd av regeringens förordningsmakt (jfr. prop. 1999/2000:25 s. 12).

Viktigt att ta i beaktande är också att syftet med en lagstiftning – att skydda den personliga integriteten – även tillgodoses genom att verksamheterna i stora delar är hemliga och att de personuppgifter som behandlas därför omgärdas av sekretess samt att verksamheterna till sin natur är sådana att det, även utan särskild lagstiftning, ställs mycket höga krav på bl.a. datasäkerhet och spridning av uppgifter till utomstående.

7.5 Grundläggande begrepp – databas eller register

Vårt förslag: Det traditionella registerbegreppet skall inte förekomma i författningarna om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. I stället skall begreppet databas användas som en rättslig beteckning på automatiserade uppgiftssamlingar som används gemensamt inom en verksamhet och för vilka särskilda handlingsregler gäller.

Databaser i stället för register

Med personregister avsågs enligt gamla datalagen register, förteckning eller andra anteckningar som förs med hjälp av automatisk databehandling och som innehåller personuppgift som kan hänföras till den som avses med uppgiften. Den i författningar allmänt använda termen för elektroniska uppgiftssamlingar har sedan datalagens införande 1973 varit register.

Det traditionella registerbegreppet har dock kritiserats vid flera tillfällen, främst eftersom det för tankarna till på visst sätt organiserade eller systematiserade samlingar av uppgifter. Detta är inte längre ett helt relevant sätt att se på samlingar av uppgifter i elektronisk form. Uppgifter kan t.ex. införas helt ostrukturerat och oorganiserat i olika filer i en dator, utan att detta förhindrar en effektiv hantering av uppgifterna för olika sammanställningar osv. Ytterligare en grund för kritik har varit att begreppet register inte används i personuppgiftslagen, som ersatt datalagen. I och för sig finns det hos flera myndigheter elektroniska samlingar av personuppgifter som enligt vår bedömning måste ses som register i ordets egentliga bemärkelse, dvs. uppgifter förs in på ett systematiserat sätt efter vissa kriterier och är sökbara endast med särskilda sökord e.d. Enligt den författning som i dag reglerar den aktuella behandlingen av personuppgifter, förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt, skall Försvarmakten föra försvarsunderrättelseregister och säkerhetsregister. Försvarets radioanstalt skall enligt samma förordning behandla personuppgifter i vissa namngivna databaser. Registerbegreppet är enligt vår uppfattning inte lämpligt när det gäller behandling av uppgifter i de datorsystem som den militära underrättelse- och säkerhetstjänsten samt Försvarets radioanstalt förfogar över och behöver för sina verksamheter. Det finns därför anledning att inte använda begreppet register i författningar om hantering av personuppgifter i myndigheternas verksamheter.

Det skulle enligt vår bedömning vara möjligt att i specialförfattningar undvika begreppet register utan att ersätta det med något specifikt alternativ, dvs. att på samma sätt som i personuppgiftslagen endast tala om behandling av personuppgifter, men det är inte självklart att det är det bästa alternativet. Att endast tala om behandling av personuppgifter kan i vissa fall föranleda att lagtexter tyngs och blir svårhanterliga, t.ex. när man inte avser behandling i allmänhet utan endast behandling i fastställda samlingar av uppgifter för vilka särskilda handlingsregler gäller. Som exempel kan nämnas att personuppgifter kan behandlas på elektronisk väg såväl med hjälp av ordbehandling vid framställning av dokument som i omfattande gemensamma informationsdatabaser. Det är inte helt enkelt att i en lag om behandling av personuppgifter klart uttrycka att man i motsvarande situationer avser att vissa bestämmelser endast skall gälla för den senare

behandlingen och inte för den tidigare, något som vi anser att det finns behov av.

Ett alternativ till registerbegreppet är termen databas, som numera förekommer i olika sammanhang, bl.a. i de författningar som gäller för hanteringen av personuppgifter inom Skatteförvaltningen och Tullverket (se prop. 2000/01:33). Vi anser att det även för Försvarmaktens och Försvarets radioanstalts verksamheter finns behov av ett särskilt begrepp för att beskriva vissa uppgiftssamlingar som är föremål för automatiserad behandling. Begreppet databas, som språkligt har mer naturlig anknytning till automatiserade sammanställningar av uppgifter, är i det här sammanhanget att föredra framför register. Begreppet databas används också, som påpekats, redan i nuvarande författning när det gäller Försvarets radioanstalts behandling av personuppgifter.

Databasbegreppet underlättar en teknikneutral lagstiftning

I våra lagförslag avser vi med begreppet databas något annat än egentliga register. En databas består av en uppgiftssamling av varierande slag, ofta rörande såväl juridiska som fysiska personer. Den kan innehålla ett antal egentliga register, men också uppgifter som inte alls kan inordnas i ett traditionellt register, såsom elektroniska färdiga handlingar i form av text eller bilder m.m. och omfattande mängder krypterade tekniska signaler. En av våra målsättningar är att skapa ett regelverk som är mer teknik neutralt än många av de registerförfattningar som finns i dag. Detta kan göras genom att begreppet databas ges en rättslig innebörd utan direkt teknisk anknytning. Vi anser att en databas skall definieras som en samling uppgifter som med hjälp av automatiserad behandling används gemensamt inom en verksamhet.

En definition av begreppet databas som den nyss angivna utesluter manuella register och gör det samtidigt möjligt att särskilja tillfälliga behandlingar av personuppgifter i en persondator från behandlingar i datorsystem som är särskilt reglerade till sitt innehåll och användningsområde. Definitionen har även den fördelen att den inte tekniskt avgränsar hur en samling uppgifter är uppbyggd eller organiserad. Det innebär att om flera register – i egentlig bemärkelse – är sammanlänkade och samtliga uppgifter i de olika registren på ett gemensamt sätt är tillgängliga för sökning med automatiserad behandling inom en avgränsad verksamhet, så utgör dessa register en databas. Med andra ord skulle automatisera-

de register kunna sägas vara en specialform av databaser, nämligen databaser vars innehåll är systematiserade på ett visst sätt enligt särskilda kriterier. En juridiskt bestämd databas kan således innehålla flera mindre databaser eller datorsystem i teknisk mening, varav en del kan vara regelrätta register. Om samtliga uppgifter i en databas finns samlade i ett enda tekniskt datorsystem eller om uppgifterna delas upp så att de rent tekniskt förvaras i olika datorsystem saknar alltså betydelse. Det väsentliga är att uppgifterna är gemensamt tillgängliga inom hela eller delar av myndigheternas verksamheter och för vilket eller vilka ändamål behandlingen sker.

Dessa tankegångar har som utgångspunkt att en lag om behandling av personuppgifter inte skall reglera hur uppgifterna tekniskt organiseras, utan endast utgöra en rättslig ram för vilka uppgifter som får behandlas och på vilket sätt de får användas, för att bl.a. säkerställa ett gott integritetsskydd. Detta innebär att regleringen av databaser i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet kan innehålla bestämmelser om behandling av samtliga de uppgifter som i dag finns i olika register och datorsystem, utan att det för den sakens skull anges hur uppgifterna skall organiseras eller delas in i grupper. Om det i en lag anges att en sådan databas får innehålla samtliga uppgifter som i dag behandlas i olika datorsystem eller register, så tar man därigenom inte ställning till den tekniska utformningen. Det kan alltså i princip bli fråga om ett stort centralt eller flera små lokalt anordnade datorsystem eller register eller en blandning av båda alternativen. Det väsentliga är att de krav lagen ställer på behandlingen för att säkerställa enskildas personliga integritet efterlevs.

8 Författningsreglering

8.1 Lagstiftningens systematik och allmänna tillämpningsområde

Vårt förslag: Den i dag gällande förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt skall ersättas av två nya lagar med tillhörande förordningar. Den ena lagen skall reglera behandlingen av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten. Den andra skall omfatta behandlingen av uppgifter i Försvarets radioanstalts underrättelseverksamhet. De nya lagarna skall ha samma inbördes systematik och delas in i tre kapitel:

- allmänna bestämmelser som i huvudsak är tillämpliga på all behandling av uppgifter som omfattas av lagen,
- särskilda bestämmelser som endast gäller automatiserad behandling av uppgifter i gemensamma databaser, samt
- bestämmelser om enskildas rättigheter vid behandlingen av personuppgifter, och om särskild granskning till skydd för de registrerades personliga integritet.

I vårt uppdrag ingår att kartlägga behandlingen av personuppgifter och analysera behovet av nya bestämmelser samt lämna förslag till sådana bestämmelser i lag. Som tidigare framhållits är det statsmakternas uppfattning att omfattande behandling av personuppgifter som dessutom kan vara av särskilt känslig natur bör regleras särskilt i lag i stället för förordning. Vi föreslår därför att den nu gällande förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt skall ersättas av en reglering i lagform. Enligt vår uppfattning skall respektive myndighets behandling av personuppgifter regleras för

sig i en särskild lag. Vi föreslår således en lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt en lag om behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet.

Det finns ingen enhetlig systematik bland de registerförfattningar som i dag gäller inom skilda myndighetsområden. Vilken systematik som väljs kan vara beroende av olika faktorer, exempelvis hur omfattande regleringen är, vilken verksamhet den avser och om författningen gäller utöver eller i stället för personuppgiftslagen. I både Försvarmaktens och Försvarets radioanstalts verksamhet behandlas en stor mängd uppgifter som ofta kan vara av känslig natur och ändamålen med verksamheterna är i stort sett desamma. Verksamheterna påminner mycket om varandra också när det gäller den säkerhet och sekretess som omgärdar behandlingen av personuppgifter.

Vi anser att de båda lagarna skall vara uppbyggda enligt samma struktur. Det innebär att det i ett första kapitel finns bestämmelser som skall tillämpas generellt på all behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten respektive Försvarets radioanstalts underrättelseverksamhet. Härigenom kommer behandling av personuppgifter att omfattas av kapitlet oavsett om det gäller e-posthantering, enkel ordbehandling eller förändret av omfattande och för myndigheten gemensamma databaser.

I ett andra kapitel återfinns regler som gäller endast för den särskilda form av automatiserad behandling av uppgifter som utförs i en databas för gemensam användning i verksamheten. I ett avslutande kapitel samlas de bestämmelser som gäller vilka rättigheter enskilda har gentemot den personuppgiftsansvariga myndigheten, dvs. Försvarmakten respektive Försvarets radioanstalt. I tredje kapitlet finns också bestämmelser om att en särskild myndighet skall ha till uppgift att granska den behandling av personuppgifter som utförs inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

8.2 Allmänna bestämmelser

8.2.1 Tillämpningsområde

Vårt förslag: Den lag som reglerar behandling av uppgifter i Försvarsmakten skall tillämpas på sådan behandling som sker i myndighetens försvarsunderrättelseverksamhet och i den militära säkerhetstjänsten. När det gäller Försvarets radioanstalt tillämpas lagen på den behandling som sker i myndighetens underrättelseverksamhet.

Lagarna skall tillämpas vid behandling av personuppgifter som är helt eller delvis automatiserad. Även behandling av personuppgifter i vissa manuella register skall omfattas av lagarnas tillämpningsområde.

De bestämmelser i lagarna som reglerar ändamålen med och ansvaret för behandlingen av uppgifter samt behandling av uppgifter i särskilda gemensamma automatiserade uppgiftssamlingar (databaser), skall vara tillämpliga även vid behandling av uppgifter om juridiska personer.

Verksamhetsområden

Den lag som reglerar behandlingen av personuppgifter inom Försvarsmakten skall omfatta sådan behandling som sker inom myndighetens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten. Lagen som reglerar viss behandling av personuppgifter inom Försvarets radioanstalt skall omfatta den behandling som sker inom myndighetens underrättelseverksamhet. Vad försvarsunderrättelseverksamhet och säkerhetstjänst samt Försvarets radioanstalts underrättelseverksamhet inbegriper för verksamhet och behandling av personuppgifter har beskrivits i kapitel 2–3 och 5–6. Begreppen försvarsunderrättelseverksamhet och militär säkerhetstjänst definieras inte särskilt i lagen, inte heller vad som inbegrips i Försvarets radioanstalts underrättelseverksamhet preciseras närmare i författningstexten. När det gäller att avgöra om en behandling omfattas av någon av de aktuella verksamheterna kan emellertid ledning hämtas från de bestämmelser i respektive författning som beskriver för vilka ändamål uppgifter får behandlas. Vad som avses med försvarsunderrättelseverksamhet och vilka myndigheter som skall bedriva denna verksamhet framgår av lagen (2000:130) om försvarsunderrättelseverksamhet och förordningen

(2000:131) om sådan verksamhet. Grundläggande författningar vad gäller militär säkerhetstjänst är säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633).

Utanför lagarnas tillämpningsområde faller behandling av personuppgifter i samband med de interna och administrativa åtgärder som kan förekomma i Försvarmaktens och Försvarets radioanstalts verksamheter. För behandling av uppgifter som rör sådana frågor, t.ex. i personal- och lönerregister, gäller i stället personuppgiftslagen. När det gäller behandling av personuppgifter om egen personal kan denna emellertid komma att omfattas av lagarnas bestämmelser om behandlingen sker för något av de ändamål som anges i lagarna. Sådan behandling kan särskilt förekomma i den militära säkerhetstjänsten som även omfattar uppgifter som rör den egna personalen.

Behandling som omfattas

Enligt vår uppfattning bör författningarna för Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt för Försvarets radioanstalts underrättelseverksamhet omfatta sådan grundläggande behandling som omfattas av personuppgiftslagen. Härmed avses helt eller delvis automatiserad behandling av personuppgifter och behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Manuell behandling i t.ex. register omfattas alltså av lagstiftningen om uppgifterna är tillgängliga för sökning eller sammanställning enligt mer än ett kriterium.

Personuppgiftslagen gäller endast vid behandling av personuppgifter, dvs. all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Det innebär att behandling av uppgifter om juridiska personer och avlidna inte alls omfattas av lagen. Försvarmakten och Försvarets radioanstalt behandlar i de aktuella verksamheterna stora mängder uppgifter som rör andra än levande fysiska personer, t.ex. företag, myndigheter och organisationer som är av intresse för svensk utrikes-, försvars- och säkerhetspolitik eller från säkerhetsskyddssynpunkt. Dessa kategorier har av naturliga skäl inte samma behov av integritetsskydd som levande fysiska personer, men det kan enligt vår uppfattning ändå finnas anledning att låta dem omfattas av regleringen när det gäller

vad myndigheterna får och inte får registrera i sina datorsystem och hur uppgifterna sedan får användas.

Vi föreslår därför att även juridiska personer skall omfattas av de bestämmelser i författningarna som anger ändamålet med och ansvaret för behandlingen. Med juridiska personer avses även myndigheter och handelsbolag. Även bestämmelser om när uppgifter behandlas i gemensamma datorsystem (se avsnitt 8.3 om databaser) skall omfatta juridiska personer.

8.2.2 Förhållandet till personuppgiftslagen

Vårt förslag: Bestämmelser i personuppgiftslagen skall tillämpas på behandling av personuppgifter inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet endast när det anges särskilt.

De bestämmelser i personuppgiftslagen som skall vara allmänt tillämpliga är de om definitioner, förhållandet till offentlighetsprincipen, grundläggande krav på behandling, säkerheten vid behandling, personuppgiftsombudets uppgifter samt tillsynsmyndighetens befogenheter och straff.

Hänvisning till personuppgiftslagen

En viktig fråga är i vilken omfattning personuppgiftslagens bestämmelser skall vara tillämpliga inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Personuppgiftslagen är generellt tillämplig på behandling av personuppgifter och den kommer därför att gälla i myndigheternas underrättelseverksamhet och säkerhetstjänst, om det inte finns avvikande bestämmelser i lag eller förordning. Som vi nämner i avsnitt 7.3 behövs det från personuppgiftslagen avvikande bestämmelser för Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet. Det innebär att det i båda lagarna som vi föreslår finns vissa uttryckliga bestämmelser som avviker från personuppgiftslagens regler. Samtidigt uppstår frågan hur man skall hantera de bestämmelser som inte skall avvika från personuppgiftslagens

regler. I tidigare lagstiftningsärenden har olika varianter förekommit.

En modell är att i en särskild författning över huvud taget inte nämna personuppgiftslagen eller klart ange att den särskilda författningen gäller utöver personuppgiftslagen. I båda fallen gäller avvikande bestämmelser i den särskilda författningen före personuppgiftslagen. När reglering i den särskilda författningen saknas kommer däremot personuppgiftslagens bestämmelser att vara tillämpliga. Nackdelen med att låta den särskilda författningen gälla utöver personuppgiftslagen är att det kan vara svårt för lagtillämparen att överblicka vilka bestämmelser i personuppgiftslagen som är tillämpliga och i vilken omfattning bestämmelserna i den särskilda författningen avviker från personuppgiftslagens regler.

En annan modell är att de bestämmelser i personuppgiftslagen som skall vara tillämpliga skrivs ut i klartext i den särskilda författningen, som alltså gäller i stället för personuppgiftslagen. Fördelen med en sådan lösning är att tillämparen snabbt får klart för sig vilka bestämmelser som gäller utan att ens behöva gå till personuppgiftslagen. En sådan modell har använts i Polisdatautredningens betänkande *Behandling av personuppgifter i polisens verksamhet* (SOU 2001:92) med förslag till ny polisdatalag. Utformningen av lagen har där motiverats med att det är en fördel för tillämparen att ha alla tillämpliga bestämmelser samlade i en enda lag. En nackdel med att skriva in bestämmelser som finns i personuppgiftslagen är att man därigenom inför en onödig dubbelreglering, eftersom personuppgiftslagens bestämmelser ändå gäller om inget annat anges. Dessutom innebär även mindre ändringar i personuppgiftslagen att motsvarande justeringar måste göras i den särskilda författningen. Den särskilda lagen kan även komma att bli onödigt omfattande till formatet.

Ett tredje sätt att utforma lagstiftningen på är att de bestämmelser som avviker från personuppgiftslagen regleras särskilt i specialförfattningen och att det uttryckligen hänvisas till de lagrum i personuppgiftslagen som skall vara tillämpliga. Även denna modell bygger på att det är av stort värde att inte lämna lagtillämparen utan vägledning när det gäller frågan om vilka bestämmelser i personuppgiftslagen som är tillämpliga. Denna metod har i och för sig fått kritik från Lagrådet som bl.a. ansåg lagstiftningstekniken riskfylld med hänsyn till såväl svårigheterna att överblicka om dataskyddsdirektivet blir tillfullo genomfört i registerlagstiftningen som till möjligheten att vid kommande

lagändringar hänvisningarna till personuppgiftslagen blir felaktiga eller missvisande (prop. 2000/01:33 s. 345f.).

Det är enligt vår uppfattning av väsentlig betydelse att inte lämna lagtillämparen utan vägledning när det gäller tolkningen av vilka bestämmelser i personuppgiftslagen som är tillämpliga. Det visar inte minst Polisdatautredningens förslag, som till stor del är en följd av de problem inom polisväsendet som orsakats av att man varit tvungen att arbeta med två lagar samtidigt (se SOU 2001:92 s. 152).

Vi förordar en lagstiftningsteknik där specialförfattningen gäller i stället för personuppgiftslagen och hänvisning görs till tillämpliga bestämmelser i personuppgiftslagen. Denna lagstiftningsteknik tillämpas också i dag, trots Lagrådets kritik, i den lagstiftning om behandling av personuppgifter som gäller inom skatteförvaltningen (SFS 2001:181–183), exekutionsväsendet (SFS 2001:184) och Tullverket (SFS 2001:185). I betänkandet Informationshantering och behandling av uppgifter vid domstolar – En rättslig översyn (SOU 2001:100) föreslår Domstolsdatautredningen att de särskilda lagreglerna för domstolarnas behandling av personuppgifter skall gälla i stället för personuppgiftslagen, med undantag för vissa bestämmelser i personuppgiftslagen som pekas ut i de särskilda lagarna. Motsvarande lagstiftningsteknik används också i Tullbrottsdatautredningens betänkande Tullverkets brottsbekämpning, Integritet – Effektivitet (SOU 2002:113). Datainspektionen har i remissyttranden förordat denna lagstiftningsteknik och framhållit att det finns ett stort värde i att lämna lagtillämparen vägledning genom att ange i speciallagen vilka bestämmelser i personuppgiftslagen som skall tillämpas. Lagstiftningstekniken har vidare den fördelen att registerlagen blir mindre omfattande och inte medför en dubbelreglering i förhållande till personuppgiftslagen. Ett antal remissinstanser som yttrat sig över Polisdatautredningens lagstiftningsteknik har också förordat en hänvisning till tillämpliga bestämmelser i personuppgiftslagen i stället för att upprepa dem i speciallagen.

Vi anser att man inte skall överdriva den av Lagrådet påtalade risken att hänvisningar kan bli felaktiga vid lagändringar, inte minst mot bakgrund av att regleringen avser ett rättsområde som har sin grund i ett EG-direktiv och därför inte kan antas komma att genomgå några större förändringar inom i vart fall den närmaste tiden. Vi har då beaktat den pågående Utredningen om översyn av personuppgiftslagen (Dir 2002:31). Dessutom bör man, som tidigare påtalats, beakta den omständigheten att den militära

underrättelse- och säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet faller inom ett rättsområde som över huvud taget inte omfattas av dataskyddsdirektivets tillämpningsområde (se avsnitt 4.4.1).

Vår bedömning är att de ovan nämnda fördelarna med en metod som innebär att våra föreslagna lagar gäller utöver personuppgiftslagen och att det ges uttryckliga hänvisningar till de bestämmelser i personuppgiftslagen som är tillämpliga mycket klart överväger nackdelarna. Vi föreslår därför att en sådan modell används i författningarna om behandling av personuppgifter inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Tillämpliga bestämmelser i personuppgiftslagen

Redovisningen nedan av vilka bestämmelser i personuppgiftslagen som vi föreslår skall vara tillämpliga vid behandling av personuppgifter i verksamhet vid Försvarmakten och Försvarets radioanstalt omfattar inte de bestämmelser som direkt rör enskildas rättigheter; information, rättelse och skadestånd. Vi föreslår att dessa bestämmelser skall återfinnas i författningarnas tredje kapitel och återkommer därför till de bestämmelserna i avsnitt 8.4.

Definitioner (3 § personuppgiftslagen)

Vi har inte funnit någon anledning att definiera de begrepp som förekommer i de av oss föreslagna författningarna på något annat sätt än vad som sker i 3 § personuppgiftslagen. Det framstår i stället tvärtom som viktigt att de begrepp som används i de olika författningarna har samma innebörd för att undvika missförstånd. Det bör dock anmärkas att personuppgiftsansvaret regleras särskilt i de föreslagna författningarna.

Förhållandet till offentlighetsprincipen (8 § personuppgiftslagen)

Bestämmelsen i 8 § första stycket personuppgiftslagen är en ren upplysning och markering av offentlighetsprincipens företräde. I andra stycket finns dock en materiell regel som anger att 9 § fjärde stycket personuppgiftslagen inte skall tillämpas i fråga om myndig-

heters användning av personuppgifter i allmänna handlingar. I bestämmelsen ställs det upp begränsningar i rätten att använda sig av personuppgifter som behandlas för historiska, statistiska eller vetenskapliga ändamål för att vidta åtgärder i fråga om den registrerade. Personuppgiftslagens bestämmelser hindrar inte heller att allmänna handlingar bevaras eller att arkivmaterial tas om hand för arkivering. Dessa undantag bör gälla även inom den militära underrättelse- och säkerhetstjänsten och i Försvarets radioanstalts underrättelseverksamhet.

Grundläggande krav på behandlingen av personuppgifter (9 § personuppgiftslagen)

En av de viktigaste bestämmelserna i fråga om behandling av personuppgifter finns i 9 § personuppgiftslagen och avser vilka grundläggande krav som ställs på en personuppgiftsansvarig (se avsnitt 4.7.2). Dessa krav bör tillämpas även vid behandling av personuppgifter inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Frågor om bevarande och gallring behandlas särskilt i avsnitt 9.1.

Säkerheten vid behandling (30 och 31 §§ personuppgiftslagen)

I 30–32 §§ personuppgiftslagen finns regler om hur den personuppgiftsansvarige skall organisera arbetet med behandlingen av personuppgifter för att garantera säkerheten. Det rör sig om instruktioner till personalen samt tekniska och organisatoriska åtgärder. I fråga om behandling av uppgifter i databaser kan det finnas behov av såväl tekniska lösningar för datorsystemen som olika behörighetsnivåer för personalkategorier, för att garantera att lagstiftningen efterlevs. Det kan diskuteras vilken funktion det fyller att för Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet hänvisa till någon av dessa bestämmelser. Den tekniska säkerheten vad gäller intrångsskydd, behörighetsnivåer för tillgång till behandlade uppgifter samt spridningsbegränsningar m.m. är av naturen av största betydelse för den militära underrättelse- och säkerhetstjänsten och Försvarets radioanstalt, redan av andra skäl än personuppgiftslagens bestämmelser.

Enligt vår uppfattning kan det emellertid finnas anledning att hänvisa till bestämmelserna om personer som behandlar personuppgifter och säkerhetsåtgärder i 31 och 32 §§ personuppgiftslagen. Härigenom understryks att säkerhet är viktigt inte bara med hänsyn till verksamheten som sådan utan också för skyddet av den personliga integriteten.

Enligt vår uppfattning är det däremot inte lämpligt att Datainspektionen skall ha befogenhet att tala om för Försvarsmakten och Försvarets radioanstalt vilka säkerhetsåtgärder myndigheten skall vidta i detta sammanhang. Bestämmelserna i 32 § personuppgiftslagen bör därför inte vara tillämpliga.

Personuppgiftsombudets uppgifter m.m. (36 § andra stycket och 38–40 §§ personuppgiftslagen)

Automatiserade behandlingar av personuppgifter skall enligt 36 § personuppgiftslagen anmälas till tillsynsmyndigheten (Datainspektionen). Anmälan behöver dock inte göras för behandlingar som regleras genom särskilda föreskrifter i lag eller förordning. Det torde inte finnas någon anledning att ställa krav på anmälningsskyldighet för behandlingar som utförs med stöd av de lagar som vi föreslår. Hänvisning görs därför inte till 36 § första stycket eller 41 § personuppgiftslagen.

Den personuppgiftsansvarige har enligt 36 § andra stycket möjlighet att utse ett personuppgiftsombud. Om ett sådant ombud utses, vilket såväl Försvarsmakten som Försvarets radioanstalt har gjort, skall bestämmelserna om ombudets skyldigheter i 38–40 §§ personuppgiftslagen tillämpas.

Bestämmelserna i 42 § personuppgiftslagen ålägger den personuppgiftsansvarige en generell skyldighet att till var och en som efterfrågar det lämna information om behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten. Upplýsingarna skall omfatta det som en anmälan enligt 36 § första stycket personuppgiftslagen annars skulle ha omfattat. Upplýsning behöver emellertid inte lämnas om uppgifter som omfattas av sekretess. I Datainspektionens föreskrifter (DIFS 1998:2) regleras vilka uppgifter en anmälan enligt 36 § första stycket skall innehålla. De flesta av dessa uppgifter är sådana som framgår av den av oss föreslagna författningstexten, t.ex. vem den personuppgiftsansvarige är och vilket ändamål behandlingen har. Övriga är sådana som i försvarsunderrättelseverksamhet och säkerhetstjänst typiskt

sett omfattas av sekretess, t.ex. upplysning om överföring till tredje land och vilka säkerhetsåtgärder som vidtagits. Med hänsyn härtill är det vår uppfattning att en hänvisning till 42 § personuppgiftslagen inte skulle vara till någon nytta för enskilda. Det skulle dessutom kunna leda till problem för de personuppgiftsansvariga myndigheterna då någon anmälningsskyldighet i övrigt inte gäller. Vi föreslår därför att 42 § personuppgiftslagen inte skall vara tillämplig.

Tillsynsmyndighetens befogenheter (43 och 47 §§ personuppgiftslagen)

För att kunna säkerställa att personuppgifter behandlas på ett korrekt sätt har Datainspektionen vissa befogenheter gentemot de personuppgiftsansvariga. Den möjlighet som inspektionen har enligt 43 § personuppgiftslagen att på begäran få tillgång till personuppgifter, upplysningar och dokumentation om behandlingen och säkerheten samt tillträde till lokaler bör gälla för de aktuella verksamheterna inom Försvarmakten och Försvarets radioanstalt.

Det anses inte möjligt för Datainspektionen (eller annan myndighet) att vid vite förbjuda en personuppgiftsansvarig statlig myndighet att behandla personuppgifter. Vite som sanktionsmedel bör enligt allmänna rättsgrundsatser inte användas mellan statliga myndigheter (jfr. Lavin, Viteslagstiftningen, s. 34ff.) Hänvisning behöver därför inte göras till bestämmelserna om vite i 44–46 §§ personuppgiftslagen.

I 45 § personuppgiftslagen anges vidare att tillsynsmyndigheten, förutom genom förbud förenat med vite, skall försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden när myndigheten konstaterar att personuppgifter behandlas felaktigt. Enligt vår uppfattning är det självklart att Datainspektionen vidtar de åtgärder som är rimliga för att få till stånd rättelse när brister i myndigheternas hantering av personuppgifter upptäcks. Det är därför inte nödvändigt att hänvisa till denna bestämmelse.

I 47 § personuppgiftslagen föreskrivs att tillsynsmyndigheten hos länsrätten får ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt skall utplånas. Denna bestämmelse bör enligt vår uppfattning gälla även i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Straff (49 §)

Personuppgiftslagens bestämmelser om straffansvar bör omfatta även verksamhet inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Bestämmelserna bör därför vara tillämpliga även när personuppgifter behandlas med stöd av de av oss föreslagna författningarna. I praktiken blir emellertid endast ett begränsat antal förfaranden straffbara, eftersom många av de bestämmelser i personuppgiftslagen som 49 § hänvisar till har undantagits från de av oss föreslagna lagarnas tillämpningsområde.

8.2.3 Personuppgiftsansvaret

Vårt förslag: Försvarmakten respektive Försvarets radioanstalt skall vara personuppgiftsansvarig för den behandling som myndigheten utför eller som det åligger den att utföra.

Försvarmakten och Försvarets radioanstalt skall vid sidan av personuppgiftsansvaret även ha ansvar för att uppgifter om juridiska personer behandlas i enlighet med de grundläggande bestämmelserna i lagstiftningen.

Personuppgiftsansvarig är enligt 3 § personuppgiftslagen den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandling av personuppgifter. I registerförfattningar är det vanligt, och enligt vår uppfattning lämpligt, att på ett tydligt sätt peka ut vem som är ansvarig för den behandling som regleras i de särskilda författningarna. För att undvika oklarheter vid den författningsreglerade behandlingen av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet bör personuppgiftsansvaret regleras uttryckligt i de särskilda författningarna.

Vi anser att personuppgiftsansvaret bör utformas så att Försvarmakten eller Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som utförs inom respektive myndighets verksamhet. Personuppgiftsansvaret innebär att den myndighet som registrerar en uppgift i t.ex. ett datorsystem har ansvaret för att uppgiften är korrekt och att den inte behandlas på ett sätt som strider mot lagstiftningen. Dessutom bör enligt vår

uppfattning personuppgiftsansvaret täcka även behandling som det åligger Försvarmakten eller Försvarets radioanstalt att utföra. På det sättet markeras att det finns ett ansvar inte endast för att utförd behandling är korrekt, utan även för att behandling faktiskt utförs när den skall ske. Som exempel på när underlåtenhet att utföra en behandling kan leda till konsekvenser för enskilda kan nämnas att en uppgift t.ex. inte gallras i föreskriven tid eller på rätt sätt.

Ansvaret för uppgifter om juridiska personer

Personuppgiftsansvaret täcker endast behandling av uppgifter om levande fysiska personer. De författningar vi föreslår är emellertid i stora delar tillämpliga även på behandling av uppgifter om juridiska personer. Det gäller de allmänna bestämmelserna om ändamål och de särskilda bestämmelserna om behandling i databaser. Av tydlighetsskäl anser vi att det därför bör framgå av lagstiftningen att myndigheternas ansvar även omfattar behandling av annat än personuppgifter. Det innebär t.ex. att Försvarmakten och Försvarets radioanstalt har ansvaret för att uppgifter om juridiska personer inte behandlas i strid med de i författningarna angivna ändamålen och att de t.ex. gallras i rätt tid. Däremot har inte juridiska personer den rätt att få information och att få uppgifter rättade som enligt personuppgiftslagen tillkommer fysiska personer. Naturligtvis bör felaktiga uppgifter om juridiska personer ändå rättas om felaktigheterna kommer till den personuppgiftsansvariges kännedom.

8.2.4 Tillåtna ändamål för behandling av uppgifter

Vårt förslag: Tydliga och konkreta ändamål för behandling av personuppgifter och andra uppgifter skall anges i lag. Uppgifter skall få behandlas automatiserat eller i manuella register endast för de angivna ändamålen.

I Försvarmaktens försvarsunderrättelseverksamhet skall uppgifter få behandlas 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.

I Försvarsmaktens militära säkerhetstjänst skall uppgifter få behandlas för att upptäcka, förebygga och avvärja säkerhets- hotande 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 säkershotande verksamhet (säkerhetsskyddstjänst), eller
3. att förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikations- och informationssystem (signalskyddstjänst).

I Försvarets radioanstalts underrättelseverksamhet skall uppgifter få behandlas 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.

Bestämmelser om för vilka ändamål uppgifter i statliga personregister får användas har alltid haft en central roll i registerförfattningar. Genom att ange ändamålen och reglera vilka uppgifter som får registreras, har ramen för hanteringen av personregister satts upp. Även om ändamålsbestämmelserna i datalagen och dataskyddskonventionen har haft stor vikt har betydelsen av klara ändamålsbestämmelser ökat än mer i och med dataskyddsdirektivet och personuppgiftslagen. Ett av de viktigaste inslagen i

direktivet är nämligen att personuppgifter får samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål samt att uppgifterna inte får behandlas för något ändamål som är oförenligt med de för vilka uppgifterna samlades in. Motsvarande bestämmelser finns i 9 § personuppgiftslagen.

Försvarsmaktens försvarsunderrättelseverksamhet

I Försvarsmaktens militära underrättelse- och säkerhetstjänst skall uppgifter få behandlas för ändamålet försvarsunderrättelseverksamhet. Med försvarsunderrättelseverksamhet avses en verksamhet eller process för att hämta in, bearbeta och delge underrättelseinformation. Försvarsunderrättelser utgörs av säkerhetspolitiska och militärstrategiska bedömningar, analyser av pågående och framtida konflikter samt biografiska underrättelser, som avser personlig information om militär personal och andra viktiga befattningshavare t.ex. politiker.

Ändamålet för behandlingen är att Försvarsmakten skall kunna utföra de uppgifter som åligger myndigheten enligt lagen (2000:130) och förordningen (2000:131) om försvarsunderrättelseverksamhet. Enligt dessa författningar åligger det Försvarsmakten att bedriva försvarsunderrättelseverksamhet för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Försvarsunderrättelseverksamhet är ett led i Försvarsmaktens uppgifter att i fred, under beredskap och i krig ge underlag för Försvarsmaktens beredskap, operativa verksamhet och förbandsproduktion samt för krigsorganisationens utveckling och materiella förnyelse (prop. 1999/200:25 s. 14). Utgångspunkten är att den militära underrättelsetjänsten skall fullgöra centrala uppgifter inom ramen för den grundberedskap som Försvarsmakten skall upprätthålla för försvar mot väpnat angrepp och för att hävda svensk territoriell integritet. Viktiga uppgifter är vidare att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred. De ökade satsningarna på internationella fredsfrämjande insatser ställer också krav på underrättelseinformation.

Försvarsmaktens försvarsunderrättelseverksamhet leds och bedrivs huvudsakligen vid Högkvarterets enhet för underrättelse- och säkerhetstjänst (MUST). För att kunna utföra alla åligganden som Försvarsmakten har på detta område bedrivs emellertid

underrättelseverksamhet även hos olika lokala och regionala organisationsenheter inom Försvarsmakten, inklusive förband i utlandsstyrkan. Sveriges försvarsattachéer vid utlandsmyndigheterna inhämtar och vidarebefordrar även de betydelsefull information för den militära underrättelse- och säkerhetstjänsten.

Som tidigare framhållits är det inte möjligt att lagreglera försvarsunderrättelseverksamhet i detalj. Detta får naturligtvis konsekvenser även för hur noggrant ändamålen för myndighetens behandling av personuppgifter inom verksamheten kan preciseras. De närmare riktlinjerna för den svenska försvarsunderrättelseverksamheten läggs fast av regeringen som anger riktlinjerna för den svenska försvarsunderrättelseverksamheten i t.ex. regleringsbrev. Inom Regeringskansliet har också inrättats en samordnande funktion för kontinuerlig inriktning av försvarsunderrättelseverksamheten genom etablerandet av en styrgrupp för säkerhetspolitiska underrättelsefrågor. Styrgruppen stöds av ett sekretariat som har till uppgift att löpande följa underrättelseverksamheten.

De uppgifter som behandlas i Försvarsmaktens försvarsunderrättelseverksamhet kan avse alla typer av uppgifter, såväl personuppgifter som andra uppgifter vilka inte alls kan hänföras till viss person. De personuppgifter som behandlas i försvarsunderrättelseverksamheten är bl.a. uppgifter om personer som verkar inom andra staters försvars- och underrättelseväsende, ledande politiska företrädare och andra opinionsbildare samt andra personer som förekommer i underrättelserapporter eller kan komma att få ett underrättelsevärde. Alla kända uppgifter om aktuella personer kan komma att behandlas. Förutom personuppgifter behandlas en mycket stor mängd information som rör t.ex. främmande makts militära stridskrafter.

Den militära säkerhetstjänsten

Uppgifter skall få behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen.

Ändamålet med behandlingen av personuppgifter inom den militära säkerhetstjänsten är att Försvarsmakten skall kunna utföra de uppgifter som åligger myndigheten enligt säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633) och 4 § 2. förordningen (2000:555) med instruktion för Försvarsmakten. Av bestämmelsen i Försvarsmaktens instruktion framgår att myndig-

heten skall leda och bedriva militär säkerhetstjänst. Den militära säkerhetstjänsten kan delas in i säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst. Säkerhetsunderrättelsetjänsten syftar till att klarlägga verksamhet som innefattar hot mot rikets säkerhet och personer med anknytning till sådan verksamhet. Inom säkerhetsskyddstjänsten vidtas olika åtgärder för att förhindra eller försvåra säkerhetshotande verksamhet. Härvid arbetar man med att förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Verksamheten syftar också till att skydda Försvarens personal, materiel och anläggningar. 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.

De ändamål för vilka personuppgifter får behandlas inom den militära säkerhetstjänsten preciseras med en särskild bestämmelse om vilka uppgiftskategorier som får behandlas i verksamheten. Uppgifter om en person får i huvudsak behandlas endast om personen misstänks för säkerhetshotande verksamhet, har lämnat uppgift om sådan verksamhet eller om uppgifterna har framkommit genom att någon genomgått en registerkontroll enligt säkerhetsskyddslagen (1996:627). Bestämmelsen motsvarar såtillvida 14 § i den nu gällande förordningen (2001:703) om viss behandling av personuppgifter inom Försvarens radioanstalt. Den av oss föreslagna paragrafen skall emellertid inte vara tillämplig på Försvarens verksamhet med signalskyddskontroll. Sådan kontroll sker ofta rutinmässigt och måste förekomma utan föregående misstanke om samband med säkerhetshotande verksamhet.

I nämnda bestämmelse har därutöver intagits integritetsskyddande regler som mer tar sikte på uppgifternas innehåll. Det föreskrivs att uppgifter om att en person kan antas ha samband med säkerhetshotande verksamhet skall förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Därutöver skall uppgifter om en person som inte misstänks för att ha utövat eller komma att utöva säkerhetshotande verksamhet få behandlas endast om det genom särskild upplysning eller på annat sätt klart framgår att sådan misstanke inte föreligger. Bestämmelserna har sin förebild i Europarådets rekommendation

(Recommendation No. R (87) 15) om användning av personuppgifter inom polissektorn. Rekommendationen innehåller speciella dataskyddsregler för personuppgifter som förs av polismyndighet med hjälp av ADB (se avsnitt 4.2). Enligt vår uppfattning har sådana bestämmelser fog för sig i den militära säkerhetstjänsten, som uppvisar vissa likheter med polisiär verksamhet och då särskilt Säkerhetspolisen.

Försvarmaktens uppgift när det gäller att leda och bedriva den militära säkerhetstjänsten är att tillvarata de säkerhetsintressen som berör Försvarmakten. Enligt bestämmelserna i säkerhetsskyddslagen (1996:627) har Försvarmakten dels en skyldighet att ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning m.m., dels ålagts vissa uppgifter, bl.a. att utöva tillsyn av säkerhetsskyddet hos vissa myndigheter.

Myndighetens verksamhet med säkerhetstjänst leds och bedrivs i stor omfattning även den vid Högkvarteret. Säkerhetstjänst bedrivs emellertid både centralt hos MUST och regionalt på militärdistriktsnivå samt på enskilda förband. Således har varje militärdistriktsområde en egen säkerhetsavdelning. Lokalt sker också bearbetning och uppföljning av lokala händelser på förbands- eller regionnivå, ofta i samarbete med polisen, när det gäller personer som är misstänkta för verksamhet som kan hota försvarets säkerhet.

Precis som inom försvarsunderrättelseverksamhet är det viktigt med samarbete med andra myndigheter. För den militära säkerhetstjänsten gäller detta främst Säkerhetspolisen. I den militära säkerhetstjänstens uppgift ingår att biträda polisen i dess arbete med skyddet av rikets säkerhet.

I den militära säkerhetstjänsten behandlas uppgifter om t.ex. personer vid andra staters underrättelseväsenden eller annan företrädare för främmande makt som bedöms kunna utgöra ett säkerhetshot och personer som deltagit eller på annat sätt har anknytning till säkerhetshotande verksamhet. Personuppgifter behandlas även i anledning av att någon varit föremål för registerkontroll enligt säkerhetsskyddslagen om denne är anställd inom Försvarmakten eller har anknytning till säkerhetsskyddad upphandling. Varje känd uppgift om aktuella personer kan komma att behandlas.

Försvarets radioanstalts underrättelseverksamhet

Försvarets radioanstalt skall precis som Försvarmakten bedriva försvarsunderrättelseverksamhet. Försvarets radioanstalts under-

rättelseverksamhet består således även den i en process för att hämta in, bearbeta och delge underrättelseinformation i syfte att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. För dessa ändamål skall Försvarets radioanstalt få behandla personuppgifter, och härvid gäller vad som ovan anförts om Försvarsmaktens försvarsunderrättelseverksamhet.

Som tidigare framhållits är Försvarets radioanstalts verksamhet såsom försvarsunderrättelseorgan inte enbart ägnad åt att klarlägga främmande maktens rent militära och försvarspolitiska förhållanden eller militära handlingsmöjligheter. Försvarets radioanstalt bedriver därför inte enbart militär underrättelsetjänst utan har även andra uppgifter, bl.a. som ett regeringens utrikes- och säkerhetspolitiska civila inhämtningsorgan. Försvarets radioanstalt är en uppdrags- tagande myndighet där framför allt regeringen och Försvarsmakten bestämmer inriktningen för underrättelseverksamheten. Försvarets radioanstalt kan emellertid också ges särskilda uppdrag att med sin tekniska expertis lämna stöd för annan myndighetsverksamhet än sådan som rör yttre hot.

Försvarets radioanstalts underrättelseverksamhet bedrivs i huvudsak genom signalspaning enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare anger. För detta ändamål skall myndigheten få behandla personuppgifter. Utöver detta grundläggande ändamål för Försvarets radioanstalts underrättelseverksamhet har emellertid myndigheten, enligt 1–3 §§ förordningen (1994:714) med instruktion för Försvarets radioanstalt, även vissa speciella uppgifter i vilka verksamheter det föreligger ett visst behov av att behandla personuppgifter. Försvarets radioanstalt skall

- följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet,
- fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten,
- utföra matematiska bedömningar av kryptosystem för totalförsvaret, samt
- biträda andra myndigheter, vid värdering, utveckling, anskaffning och drift av signalspaningssystem.

De uppgifter som Försvarets radioanstalt behandlar i sin underrättelseverksamhet är information av betydelse för bedömningar av den allmänna utrikes och försvarspolitiska utvecklingen samt internationella relationer, krishärdar och de internationella uppdrag i vilka svensk personal deltar. Därutöver delges viss

information rörande terrorism, expertkontroll, protokollära ärenden och händelser i närheten av svenskt territorium.

Rapporteringen av underrättelser från Försvarets radioanstalt kan t.ex. röra främmande stridskrafterns rörelser, övningar och prov av vapen samt kränkningar av svenskt territorium. I underrättelseverksamheten ingår också rapportering av biografiska underrättelser. De personuppgifter som behandlas i underrättelseverksamheten är bl.a. uppgifter om personer som verkar inom andra staters försvars- och underrättelseväsenden, ledande politiska företrädare och andra opinionsbildare samt andra personer som förekommer i underrättelserapporter eller kan komma att få ett underrättelsevärde. Alla kända uppgifter om aktuella personer kan komma att behandlas.

På uppdrag av Försvarmakten och då främst den militära underrättelse- och säkerhetstjänsten (MUST), den Operativa insatsledningen (OPIL) samt Totalförsvarets forskningsinstitut (FOI) och Försvarets materielverk (FMV) behandlas främst uppgifter rörande den militära situationen i Sveriges närområde. Vidare förmedlas information om de internationella uppdrag i vilka svensk personal deltar samt om frågor rörande spridning av massförstörelsevapen, betydelsefulla vapen eller 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.

8.2.5 Behandling av känsliga personuppgifter

Vårt förslag: Uppgifter om en person skall inte få 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 skall de emellertid få kompletteras med känsliga personuppgifter, när det är nödvändigt för syftet med behandlingen.

Vid all behandling av personuppgifter intar frågor om behandling av känsliga personuppgifter enligt personuppgiftslagen en särställ-

ning, genom att sådana uppgifter i princip får behandlas endast efter samtycke av den enskilde eller med särskilt författningsstöd. Allmänt gäller att stor försiktighet bör iakttagas vid hanteringen av känsliga personuppgifter. Med känsliga personuppgifter avses uppgifter som avslöjar en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Om sådana uppgifter måste behandlas i offentlig verksamhet utan samtycke behövs det särskilda och avvikande bestämmelser för i vilka fall det får göras om inte någon av undantagsbestämmelserna i personuppgiftslagen är tillämpliga.

Vi anser att Försvarmakten och Försvarets radioanstalt i de aktuella verksamheterna bör ha samma möjligheter att registrera och på annat sätt behandla sådana uppgifter som myndigheterna har i dag. Vi föreslår därför att uppgifter om en person inte får 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. Det innebär exempelvis att det inte är tillåtet att i underrättelseverksamhet föra register över, eller på annat sätt göra anteckningar om, enskilda personer enbart på den grunden att de tillhör en viss etnisk grupp. Om uppgifter om en person däremot behandlas på annan grund måste de få kompletteras med känsliga personuppgifter när det är nödvändigt för syftet med behandlingen.

Att behandla känsliga personuppgifter kan t.ex. bli nödvändigt inom ramen för Sveriges deltagande i internationella fredsbevarande och humanitära insatser. Här bidrar såväl den militära underrättelse- och säkerhetstjänsten som Försvarets radioanstalt med underrättelser. I dessa uppdrag ingår ofta att skydda en viss minoritet. För att de svenska enheterna inom en sådan mission skall kunna utföra sina uppgifter kan det därför vara nödvändigt att uppgifter behandlas rörande t.ex. etnisk härkomst eller religiös övertygelse. Även i övrigt finns det dock ett behov av att kunna behandla känsliga uppgifter. Ofta är just det faktum att en person tillhör ett politiskt parti eller annan organisation av grundläggande betydelse från försvarsunderrättelse- eller säkerhetssynpunkt. En sådan omständighet får dock aldrig utgöra ensam grund för behandlingen.

Vi anser att en bestämmelse om känsliga personuppgifter skall vara generell, dvs. den bör gälla såväl för behandling i myndigheternas olika databaser som för annan behandling. Det bör inte heller spela någon roll för vilka ändamål uppgifterna behandlas,

utan samma regler skall gälla för försvarsunderrättelseverksamhet som för militär säkerhetstjänst.

Bestämmelserna innebär naturligtvis också en begränsning av vilka sökord som får användas vid arbete i myndigheternas databaser. Sökning är som varje annan åtgärd som vidtas i fråga om personuppgifter en behandling. Att uteslutande använda sökbegrepp som beskriver t.ex. sexualliv eller religiös övertygelse, ensamma eller i kombination med varandra, är således inte tillåtet utan annan uttrycklig grund för en sådan behandling (se vidare i avsnitt 8.3.5).

I detta sammanhang bör nämnas något om hur bestämmelsen om känsliga personuppgifter förhåller sig till den information som Försvarets radioanstalt inhämtar genom signalspaning och som lagras i den s.k. Källdatabasen. Vid inhämtning genom signalspaning sker vanligtvis inget urval, utan databasen tillförs främst obearbetad information. Källdatabasen är på så sätt endast "en spegling" av förekommande signaler. I dessa signaler kan det dölja sig information om enskilda personer och denna information kan också till viss del bestå av känsliga personuppgifter.

Den information som lagras i Källdatabasen inhämtas automatiskt och myndigheten har ofta ingen möjlighet att påverka innehållet i den eller att vid själva inhämtningen veta vilken information det insamlade materialet innehåller. Till detta kommer att materialet ofta kan vara såväl krypterat som avfattat på ett främmande språk. Det är i detta sammanhang inte möjligt för myndigheten att "censurera" innehållet i information som på detta sätt kommer in i elektronisk form genom att ta bort eventuella känsliga personuppgifter. Fråga är då om denna behandling strider mot bestämmelsen i 1 kap. 6 § i författningsförslaget.

Enligt vår uppfattning måste bestämmelsen om behandling av känsliga personuppgifter tillämpas på varje enskild behandling för sig. Inhämtning genom signalspaning är en sådan enskild behandling. Vid denna inhämtning finns över huvud taget inget syfte att behandla känsliga personuppgifter, eftersom informationen i detta led av processen ännu är helt okänd. Inhämtningen sker endast för att myndigheten skall uppfylla sin grundläggande uppgift att genom signalspaning bedriva underrättelseverksamhet. Informationen måste naturligtvis få lagras i den form den kommer in för att signalspaningen skall uppfylla sitt ändamål, oavsett om den eventuellt innehåller känsliga personuppgifter eller inte. Vi anser således att inhämtning av okänd information genom signalspaning

inte strider mot bestämmelsen om behandling av känsliga personuppgifter.

Efter att uppgifterna lagrats i källdatabasen och en vidare behandling skall ske gäller däremot bestämmelsen i 1 kap. 6 § om att känsliga personuppgifter endast får behandlas som ett komplement till andra för verksamheten nödvändiga uppgifter. Uppgifterna får då inte bearbetas vidare utan att det finns en annan uttrycklig grund för en sådan behandling. Det är också först i och med att uppgifterna behandlas vidare och analyseras som de eventuella känsliga personuppgifterna blir kända och en risk för intrång i den personliga integriteten föreligger.

8.2.6 Överföring av personuppgifter till tredje land

Vårt förslag: Personuppgifter som behandlas med stöd av lagen om behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten eller motsvarande lagstiftning när det gäller Försvarets radioanstalts underrättelseverksamhet får lämnas ut till andra länder om sekretess inte hindrar det och det behövs för att myndigheten skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet eller det annars är nödvändigt för verksamheten.

I avsnitt 9.2.2 konstaterar vi att det inte behövs någon särskild författningsreglering enbart på den grunden att uppgifter lämnas ut på medium för automatiserad behandling. Huruvida utlämnande av uppgifter skall ske bör avgöras av de förutsättningar som ges av reglerna om sekretess samt ändamålen med verksamheten.

I ett avseende fordras emellertid särskild författningsreglering, på grund bestämmelserna i Europarådets dataskyddskonvention, och det gäller överföring av personuppgifter till andra länder.

Enligt 33 § personuppgiftslagen får personuppgifter som är under behandling inte föras över till tredje land om inte det mottagande landet har en adekvat nivå för skyddet av personuppgifter. Med tredje land avses en stat som inte ingår i Europeiska unionen (EU) eller är ansluten till Europeiska ekonomiska samarbetsområdet. Från förbudet finns vissa undantag i 34 §, bl.a. för överföring till länder som har anslutit sig till Europarådets dataskyddskonvention. Enligt 35 § andra stycket personuppgifts-

lagen har regeringen, och Datainspektionen (jfr. 14 § personuppgiftsförordningen), möjlighet att föreskriva om undantag från förbudet i 33 §, om det behövs med hänsyn till ett viktigt allmänt intresse eller om det finns tillräckliga garantier till skydd för de registrerades rättigheter. Som alternativ till att regeringen föreskriver om ett generellt undantag från förbudet mot överföring av personuppgifter till tredje land kan riksdagen i lag besluta att personuppgiftslagens regler i detta avseende inte skall vara tillämpliga på den militära underrättelse- och säkerhetstjänsten. Våra författningsförslag gäller i stället för personuppgiftslagen och någon hänvisning till personuppgiftslagens regler om överföring av personuppgifter till tredje land görs inte. Härigenom blir personuppgiftslagens regler om förbud mot utlämnande av personuppgifter till tredje land inte tillämpliga vare sig i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten eller i Försvarets radioanstalts underrättelseverksamhet.

Bestämmelser om överföring av personuppgifter till andra länder finns emellertid numera även i Europarådets dataskyddskonvention, genom ett tilläggsprotokoll som Sverige undertecknade den 8 november 2001. Enligt artikel 2 första punkten i tilläggsprotokollet skall varje part endast möjliggöra överföring av personuppgifter till en mottagare som lyder en stats eller en organisations jurisdiktion som inte är part i konventionen, om staten eller organisationen tryggar en tillräcklig grad av skydd för den avsedda uppgiftsöverföringen. Som undantag från första punkten får en part tillåta överföring om det är tillåtet enligt den nationella lagstiftningen på grund av den registrerades särskilda intressen, eller när legitima intressen överväger, i synnerhet viktiga allmänna intressen.

Utlämnande av uppgifter till tredje land kan för Försvarmaktens och Försvarets radioanstalts del ske såväl inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet som vid deltagandet i internationella fredsfrämjande och humanitära insatser. Utbyte av information med utländska underrättelse- och säkerhetstjänster utgör en av grundprinciperna för försvarsunderrättelseverksamheten. Även för den militära säkerhetstjänsten skall samarbete med andra länder och internationella organisationer vara en naturlig del av verksamheten. Regeringen har i regleringsbrev uttalat att ett utbyte av information är nödvändigt för att Sverige skall kunna få del av sådan information som landet behöver men som kräver resurser som saknas. Detta ställer särskilda krav på den militära underrättelse- och säkerhetstjänsten.

Sveriges allt bredare medverkan i det internationella försvarsunderrättelse- och säkerhetssamarbetet kräver att statsmakterna genom underrättelsetjänsten får erforderlig information att lägga till grund för konfliktförebyggande åtgärder, krishantering, planering och beslut om insats. Vidare krävs att information kan lämnas som stöd för insatsstyrkornas säkerhet och operationer i missionsområdet. Underrättelsefunktionen är en förutsättning för styrkornas säkerhet, för deras förmåga att lösa sina uppgifter, för kontroll av bevakningsområdet och för att kunna leda lokala förhandlingar. I krislägen då internationella insatser övervägs krävs också snabba konsultationer mellan alla de stater och organisationer som överväger att delta (jfr. prop. 20001/02:10 s. 245f.).

Dessa omständigheter visar på betydelsen av att uppgifter kan lämnas ut till andra länder och internationella organisationer, även om det medför en överföring av personuppgifter till ett tredje land enligt personuppgiftslagen eller en mottagare som inte lyder under dataskyddskonventionens jurisdiktion. Det framstår som omöjligt att inom ramen för våra författningsförslag förutse när eller på vilket sätt som uppgifter i de aktuella verksamheterna behöver sändas till andra länder. Det bör endast vara försvars- och säkerhetspolitiska skäl som avgör detta. Vid utlämnande av uppgifter till utlandet tillämpar Försvarmakten och Försvarets radioanstalt vidare mycket stränga säkerhetskrav för att skydda sin egen verksamhet. Härigenom fungerar myndigheternas egna föreskrifter som skydd för den personliga integriteten. Mot bakgrund härav bör personuppgiftslagens och dataskyddskonventionens regler om förbud mot överföring av personuppgifter till tredje land inte vara tillämpliga varken i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten eller i Försvarets radioanstalts underrättelseverksamhet.

Undantag från dataskyddskonventionens bestämmelser om gränsöverskridande flöden av personuppgifter kräver emellertid att det är tillåtet enligt den nationella lagstiftningen bl.a. på grund av att legitima intressen överväger, i synnerhet viktiga allmänna intressen. Enligt vår uppfattning utgör möjligheten att inom det internationella försvarsunderrättelse- och säkerhetssamarbetet samt i den militära underrättelse- och säkerhetstjänstens och Försvarets radioanstalts verksamhet i övrigt lämna ut uppgifter till andra länder ett sådant viktigt legitimt allmänt intresse. Vi föreslår därför att det i lagarna avseende behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelse-

verksamhet införs en bestämmelse som medger att personuppgifter förs över till annat land.

Avsikten är att bestämmelsen inte på något sätt skall vara begränsande när det gäller myndigheternas möjligheter att lämna ut uppgifter inom ramen för det internationella underrättelse- och säkerhetssamarbetet. Det är vår uppfattning att de bestämmelser om sekretess och krav på säkerhet i övrigt som gäller för verksamheterna i detta sammanhang tillgodoser skyddet för den personliga integriteten i tillräcklig mån. Huruvida ett utlämnade skall ske eller inte måste i sin helhet avgöras efter försvars- och säkerhetspolitiska överväganden. Den bestämmelse vi föreslår har inte som syfte att ha en sekretessbrytande verkan (jfr. avsnitt 9.2.1), utan uppfyller endast de krav på nationell lagstiftning som dataskyddskonventionen ställer när det gäller överföring av personuppgifter till andra länder.

8.3 Behandling av uppgifter i databaser

8.3.1 Begreppet databas

Vårt förslag: Olika regler skall gälla för Försvarsmaktens respektive Försvarets radioanstalts behandling av uppgifter beroende på om

- behandlingen är automatiserad och utförs i en särskild samling av uppgifter som används gemensamt i verksamheten (databaser), eller
- behandlingen utförs på annat sätt av enskilda tjänstemän och uppgifterna inte görs tillgängliga för gemensam användning i verksamheten.

Som tidigare konstaterats utgör användningen av datorer sedan många år ett naturligt och omfattande inslag i den militära underrättelse- och säkerhetstjänstens arbete. För Försvarets radioanstalts underrättelseverksamhet är hantering av uppgifter den helt dominerande arbetsmetoden. Samtidigt pågår hela tiden en utveckling mot allt mer avancerade datorsystem inom de båda myndigheternas verksamheter.

Enligt vår mening måste det för Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet finnas särskilda

regelverk för den i verksamheterna helt dominerande automatiserade och gemensamma behandling av personuppgifter som inte utgörs av vanlig ordbehandling och som inte är av helt tillfällig natur. De stora gemensamma uppgiftssamlingar hos statliga myndigheter som dagens personregister utgör innebär, på grund av de tekniska möjligheterna att söka i materialet och göra sammanställningar om registrerade personer, en påtaglig risk för otillbörliga intrång i enskildas personliga integritet. Den risken blir än större ju mer avancerade system som utvecklas. Från integritetssynpunkt finns det därför enligt vår uppfattning starka skäl för att skapa tydliga regler om vad som är tillåtet i fråga om sådan behandling.

I och med genomförandet av dataskyddsdirektivet i svensk lagstiftning har den rättsliga begreppsapparaten vid datoranvändning ändrats. I personuppgiftslagen talas det inte längre om förande av personregister som i datalagen, utan om behandling av personuppgifter. För att särskilja den rättsliga regleringen av sådan automatiserad behandling som i dag görs i uppgiftssamlingar för gemensamt bruk, t.ex. personregister, från den automatiserade behandlingen av uppgifter i allmänhet, t.ex. ordbehandling och vanlig e-posthantering, har vi valt att införa det rättsliga begreppet databas i lagstiftningen (se avsnitt 7.5).

Gränsdragningen mellan gemensam behandling i en databas och annan behandling av uppgifter

För att begreppet databas skall vara praktiskt användbart på vissa särreglerade uppgiftssamlingar hos Försvarmakten och Försvarets radioanstalt, krävs att det är möjligt att avgöra var gränslinjen går mellan behandling i en databas och annan behandling, t.ex. vanlig ordbehandling. En grundläggande förutsättning för att en elektroniskt lagrad uppgift skall anses ingå i en databas, är enligt vår mening att uppgiften används gemensamt i en viss verksamhet för de ändamål som styr behandlingen av uppgifter inom verksamheten. Det väsentliga är inte på vilket sätt uppgiften tekniskt lagras, utan den faktiskt åsyftade tillgängligheten.

Det avgörande för om en uppgift används gemensamt och därmed utgör en beståndsdel i en databas, är således om den behandlas på ett sätt som medför att den utgör "allmän egendom" i verksamheten. Att olika personalkategorier kan ha olika behörighet och att vissa uppgifter därför i praktiken är åtkomliga endast för ett

begränsat antal personer inom underrättelseverksamheten eller säkerhetstjänsten, förtar enligt vår uppfattning i sig inte uppgifternas egenskap som gemensamma.

En uppgift som lagras elektroniskt på hårddisken i en dator eller i en server hos Försvarmakten eller Försvarets radioanstalt i samband med att en tjänsteman arbetar med ordbehandling, och som normalt är åtkomlig endast för tjänstemannen själv och exempelvis systemadministratören vid myndigheten, kan däremot inte anses vara gemensamt tillgänglig. Syftet med sådan tillfällig behandling är inte att uppgifterna som lagras i datorn skall användas av andra än den som utför behandlingen. Det förhållandet att systemadministratören – eller en annan tjänsteman vid myndigheten – kan få åtkomst till uppgiften genom ett visst tekniskt förfarande, kan inte anses innebära att uppgiften som sådan är lagrad för att användas gemensamt i verksamheten. Inte heller innebär det förhållandet att en uppgift behandlas tillfälligt i en dator med det uttalade syftet att den senare skall "matas in" i systemet och göras gemensam, att den är en del av databasen. Däremot kommer uppgiften att omfattas av det särskilda regelverket för en databas när den väl är registrerad i det gemensamma systemet. Ett exempel på en sådan situation kan i Försvarmaktens verksamhet vara uppgifter hämtade från Informationsdatabasen som tillsammans med annan information bearbetas med hjälp av ordbehandling av en enskild tjänsteman och som efter sammanställning registreras i Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK).

Det är inte möjligt att i lagstiftningen dra någon exakt gräns för när en viss behandling skall anses ske i en databas och därmed omfattas av det särskilda regelverket för denna. Inte minst beror detta på att det inte är möjligt att förutse den tekniska utvecklingen inom datorområdet och de möjligheter som kan öppna sig i fråga om informationsöverföring. Enligt vår uppfattning måste det från fall till fall avgöras om uppgifter som behandlas automatiserat är gemensamma eller inte. Svårigheterna med att göra den bedömningen skall dock inte överdrivas.

I de flesta fall ser vi inga problem med att bedöma om en uppgift behandlas gemensamt eller inte. En tjänsteman inom Försvarmakten eller Försvarets radioanstalt kan utan svårigheter avgöra om han eller hon för tillfället arbetar med uppgifter direkt i en särskilt reglerad databas eller med uppgifter i ett ordbehandlingsdokument. Den personuppgiftsansvarige har naturligtvis också ett ansvar för att gränsdragningsproblem inte uppstår på grund av brister i den

tekniska utformningen av ett datorsystem. De säkerhetskrav som omgärdar Försvarmaktens och Försvarets radioanstalts datorsystem i detta sammanhang medför även de att några tvivel inte bör uppstå om huruvida en viss uppgift ingår i en databas eller inte.

Sammanfattningsvis är det enligt vår mening en grundläggande förutsättning för att elektroniskt lagrade uppgifter skall anses ingå i en databas, att uppgifterna av Försvarmakten eller Försvarets radioanstalt används gemensamt i en viss verksamhet för de ändamål som skall styra behandlingen av uppgifter inom verksamheten.

För den resterande behandlingen av uppgifter är enligt vår uppfattning de grundläggande bestämmelserna i 1 kap. tillräckliga. Det gäller alltså sådan mer tillfällig behandling som sker för den enskilde tjänstemannens bruk eller behandling av uppgifter som i vart fall inte används gemensamt i underrättelseverksamheten.

8.3.2 Försvarets radioanstalts databaser

Vårt förslag: I Försvarets radioanstalts underrättelseverksamhet skall det finnas ett antal skilda samlingar uppgifter som med hjälp av automatiserad behandling används gemensamt i verksamheten (databaser).

Det skall finnas en *urvalsdata*bas för planering och inriktning av inhämtning av information. Det skall finnas en *källdata*bas för uppgifter som samlats in genom signalspaning och en *databas för öppna källor* för uppgifter som samlats in på annat sätt. För analys och bearbetning av insamlade uppgifter skall det finnas en *analysdata*bas. Underrättelserapporter skall för delgivning samlas i en *rapportdata*bas.

Som framgår av avsnitt 8.3.1 föreslår vi att det för de verksamheter vi har att utreda skall finnas en särskild reglering för den behandling av personuppgifter som sker i myndigheternas olika databaser. Vår utgångspunkt har härvid varit att det är myndigheternas behov av uppgifter i respektive verksamhet som skall vara styrande, samtidigt som det naturligtvis måste beaktas att de registrerades personliga integritet inte otillbörligen skall kränkas.

För att på ett rationellt sätt kunna hantera den mycket omfattande och komplexa informationsmängd som samlas in i Försvarets radioanstalts underrättelseverksamhet sker bearbetning och analys med hjälp datorer. Verksamheten utmärker sig på så sätt

att så gott som all behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet sker datoriserat i myndighetens databaser. Myndigheten för inga manuella register och behandling sker heller inte i fristående persondatorer.

Redan av bestämmelserna i 1 kap. förslaget till lag om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet om ändamål m.m. följer att Försvarets radioanstalt kan lägga upp speciella databaser för behandling av personuppgifter. En sådan omfattande behandling av personuppgifter, som sker i myndighetens underrättelseverksamhet och i vilken verksamhet uppgifterna dessutom är gemensamt tillgängliga för flera personer, bör enligt vår uppfattning av integritetsskäl omgärdas av vissa särskilda bestämmelser. Särskilda bestämmelser för myndighetens databaser fyller också den funktionen att det för enskilda blir tydligt vilka databaser myndigheten har och vilken behandling av uppgifter som förekommer i databaserna.

Vi anser därför att det utöver de grundläggande bestämmelserna om ändamål m.m., som är tillämpliga på all behandling av personuppgifter, skall finnas särskilda bestämmelser för sådan automatiserad behandling av personuppgifter som inte utgörs av vanlig ordbehandling e.d. och som inte är av helt tillfällig natur. Det bör finnas regler om vilka databaser som får finnas i verksamheten och för vilka särskilda ändamål uppgifter får behandlas i respektive databas. Vidare bör det finnas vissa bestämmelser om innehåll i databaserna och om begränsningar av vilka sökord som får användas samt om vilka andra myndigheter som får ha direktåtkomst till databaserna.

Försvarets radioanstalts system för behandling av personuppgifter i dess underrättelseverksamhet är helt anpassat till underrättelseprocessen. I enlighet härmed skall det enligt vår mening för inriktning av myndighetens underrättelseverksamhet finnas en urvalsdatas. Information som hämtas in skall vidare lagras i en källdatas eller datas för öppna källor. Bearbetning och analys av inhämtad underrättelseinformation skall ske i en analysdatas och underrättelserapporterna som är färdiga för delgivning skall slutligen enligt vår uppfattning lagras i en rapportdatas.

Vi anser att följande skall gälla för databaserna.

Urvalsdatatabasen – planering och inriktning

I urvalsdatatabasen skall de uppgifter behandlas som används för planering och inriktning av underrättelseverksamheten, på såväl lång som kort sikt. 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 genom de uppdrag som Försvarsmakten ger myndigheten.

I datatabasen får behandlas de sökord i form av olika personuppgifter, t.ex. personnummer och namn, som används i underrättelseverksamheten vid sökning genom signalspaning och i öppna källor. Spaning sker även efter vissa tekniska parametrar, vilka även de kan återfinnas i urvalsdatatabasen. Med parametrar avses såväl manuella som automatiska frekvenser, e-postadresser och telefonnummer.

Källdatabasen – inhämtning genom signalspaning

I källdatabasen skall all information som Försvarets radioanstalt inhämtar genom signalspaning samlas. I datatabasen samlas obearbetad information som endast är "en spegling" av förekommande signaler samt den signalspaningsinformation som inhämtats med hjälp av särskilt utvalda sökkriterier. Det inhämtade materialet kan vara såväl krypterat som avfattet på ett främmande språk.

Uppgifter som lagras i datatabasen får behandlas i den för att underlätta sökning efter information. I övrigt får uppgifterna endast behandlas genom att de förs över till analysdatatabasen. Så sker efter att en handläggare med hjälp av olika sökord funnit den information som bedöms vara intressant i underrättelseverksamheten.

Databasen för öppna källor – inhämtning på annat sätt än genom signalspaning

I datatabasen för öppna källor får Försvarets radioanstalt samla information som hämtats in på annat sätt än genom signalspaning. Sådan insamling sker t.ex. genom prenumeration på utländska tidningar, sökning av information på Internet eller helt enkelt genom riktad inhämtning av uppgifter från olika webbsidor.

Uppgifter som lagras i databasen får behandlas för att underlätta sökning efter information. I övrigt får uppgifterna endast behandlas genom att de förs över till analysdatabasen. Överföring sker efter att en handläggare med hjälp av olika sökord funnit information som bedöms vara intressant i underrättelseverksamheten.

Analysdatabasen – bearbetning och analys

I analysdatabasen får de uppgifter behandlas som överförts från källdatabasen och databasen för öppna källor. Även annan för underrättelseverksamheten nödvändig information får behandlas i databasen. I databasen sker analys och annan bearbetning, såsom dekryptering och översättning, av den information som Försvarets radioanstalt hämtat in genom signalspaning och från öppna källor.

I analysdatabasen får informationen som undergår analys och bearbetning lagras fram till dess den färdigställs till underrättelse-rapporter och lagras i rapportdatabasen.

Rapportdatabasen – delgivning

Rapportdatabasen får endast innehålla Försvarets radioanstalts färdiga underrättelserapporter som skall delges uppdragsgivarna. I rapporterna finns de underrättelser som framtagits genom analys och bearbetning i analysdatabasen.

8.3.3 Försvarsmaktens databaser

Vårt förslag: I Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst skall det finnas ett antal skilda samlingar uppgifter som med hjälp av automatiserad behandling används gemensamt i verksamheterna (databaser). Det skall finnas en *informationsdatabas* samt en *underrättelse- och säkerhetsdatabas*.

Även i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten sker omfattande behandling av personuppgifter i särskilda databaser. Till skillnad mot vad som är fallet i Försvarets radioanstalts underrättelseverksamhet sker i den militära underrättelse- och säkerhetstjänsten även behandling utanför dessa

databaser, i enskilda personatorer och till och med rent manuellt. Det föreligger emellertid en sådan omfattande behandling av gemensamt tillgängliga personuppgifter i den militära underrättelse- och säkerhetstjänsten att det även i dessa verksamheter bör finnas vissa särskilda bestämmelser till skydd för den personliga integriteten. Såväl Försvarets radioanstalt som Försvarmakten bedriver försvarsunderrättelseverksamhet och de båda myndigheternas verksamhet uppvisar härvid vissa likheter. Det är med hänsyn härtill befogat att ha samma struktur när det gäller regleringen av behandling av personuppgifter.

Vi föreslår därför att det i lagen om behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten, utöver de grundläggande bestämmelserna om ändamål m.m. som är tillämpliga på all behandling av personuppgifter, skall finnas särskilda bestämmelser för sådan automatiserad behandling av personuppgifter som inte utgörs av vanlig ordbehandling e.d. och som inte är av helt tillfällig natur. Det bör finnas regler för vilka databaser som får finnas i verksamheten och för vilka särskilda ändamål uppgifter får behandlas i respektive databas. Vidare bör det finnas vissa bestämmelser om innehåll i databaserna och om begränsningar av vilka sökord som får användas samt om vilka andra myndigheter som får ha direktåtkomst till databaserna.

Inom den militära underrättelse- och säkerhetstjänsten finns det två typer av register eller databaser, antingen för öppen eller hemlig information. Information som inte är hemlig samlas i en särskild informationsdatabas. Hemliga uppgifter lagras i olika databaser anpassade till ändamålet med den särskilda behandlingen. Den viktigaste databasen är härvid Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK). Det finns även vissa andra databaser för behandling av hemlig information, bl.a. BANIO som används för bearbetning och analys vid internationella operationer samt MINSK som används för kommunikation med Sveriges försvarsattachéer (se avsnitt 5.3). Vårt förslag till reglering av Försvarmaktens databaser i den militära underrättelse- och säkerhetstjänsten följer denna indelning med databaser för öppen respektive hemlig information.

Vi anser att följande bör gälla för databaserna.

Informationsdatabasen

I informationsdatabasen får Försvarsmakten samla information som inhämtats från öppna källor. I databasen lagras information som samlats in via sökning på Internet och i viss mån från litteratur och tidskrifter. Uppgifter hämtas också in på automatiserad väg från kommersiella nyhetsleverantörer.

Information som lagras i databasen får behandlas i den för att underlätta sökning efter den information som hämtats in från öppna källor. I övrigt får uppgifterna endast behandlas genom att föras över till underrättelse- och säkerhetsdatabasen.

Underrättelse- och säkerhetsdatabasen

I underrättelse- och säkerhetsdatabasen skall i första hand samlas sådan information som samlats in från andra än öppna källor, dvs. hemliga och kvalificerat hemliga uppgifter. Trots likheten i namn avses med underrättelse- och säkerhetsdatabasen inte enbart IS UNDSÄK. Det rättsliga begreppet underrättelse- och säkerhetsdatabas är avsett att vara ett samlande namn för alla de olika databaser där Försvarsmakten behandlar hemliga uppgifter för ändamålen försvarsunderrättelseverksamhet och militär säkerhetstjänst. Som exempel på sådana databaser kan som ovan angivits nämnas IS UNDSÄK, BANIO och MINSK.

Som tidigare framhållits är begreppet databas i detta sammanhang inte ett tekniskt begrepp utan en rättslig beteckning, på vissa automatiserade uppgiftssamlingar vilka används gemensamt i verksamheten och för vilka samma regler skall gälla. Den rättsliga beteckningen databas kan således omfatta flera mindre register, databaser eller datorsystem i teknisk mening. Om uppgifterna finns samlade i ett enda tekniskt system eller om uppgifterna delas upp så att de rent tekniskt förvaras i olika datorsystem saknar betydelse. Det väsentliga är i detta sammanhang att uppgifterna är gemensamt tillgängliga inom hela eller delar av den militära underrättelse- och säkerhetstjänstens verksamhet. Denna reglering faller tillbaka på våra grundläggande tankegångar om att en lag om behandling av uppgifter inte skall reglera hur uppgifterna tekniskt organiseras utan endast utgöra en rättslig ram för vilka uppgifter som får behandlas och på vilket sätt de får användas. En sådan reglering medför också att nya och mer tekniskt utvecklade system kan skapas i framtiden utan att lagtekniska hinder sätter stopp för

det. Det avgörande är härvid att behandlingen av personuppgifter endast sker för de särskilt fastställda ändamålen och i enlighet med lagens regler i övrigt.

I underrättelse- och säkerhetsdatabasen får uppgifter behandlas som samlats in från andra än öppna källor. I databasen får också behandlas uppgifter som överförts från informationsdatabasen av den anledningen att uppgifterna ansetts vara av intresse i den militära underrättelse- och säkerhetstjänsten.

Information som lagras i underrättelse- och säkerhetsdatabasen får behandlas för att underlätta sökning efter uppgifter som samlats in från såväl öppna som hemliga källor i den militära underrättelse- och säkerhetstjänsten. I databasen får vidare analys och bearbetning av inhämtat underrättelsematerial ske och färdiga underrättelse-rapporter lagras och delges inom systemet.

8.3.4 Uppgifter som får behandlas

Vårt förslag: Regeringen, eller den myndighet som regeringen bestämmer, meddelar närmare föreskrifter om vilka uppgifter som får behandlas i Försvarets radio- och radioanstalts databaser.

I förordning införs vissa bestämmelser om vilka uppgifter som får behandlas i databaserna.

I avsnitt 7.4 diskuterar vi frågan om detaljreglering av vilka uppgifter som får behandlas automatiserat i Försvarets radio- och radioanstalts underrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Vi redovisar där som vår inställning att den främsta uppgiften för en lag om behandling av uppgifter bör vara att slå fast grundläggande principer för behandlingen och inte att i detalj reglera vad som får registreras. Det främsta skälet för en sådan ordning är att verksamheterna är av sådan art att det inte är möjligt att i lagform reglera behandlingen av uppgifter i detalj. Att beakta i detta sammanhang är även att det grundläggande syftet med lagstiftningen – att skydda den personliga integriteten – även tillgodoses genom att verksamheterna i stora delar är hemliga och att de personuppgifter som behandlas därför omgärdas av sekretess. Verksamheterna är dessutom till sin natur sådana att det, även utan särskild lagstiftning, ställs mycket höga krav på bl.a. datasäkerhet

och spridning av uppgifter till utomstående. För att en detaljreglering av innehållet i en databas skall kunna undvikas krävs dock enligt vår uppfattning att de ändamål för vilka uppgifter får behandlas är tydliga och konkreta (se avsnitt 7.2).

Vi har mycket noggrant utrett möjligheterna att närmare reglera vilka uppgifter myndigheternas databaser skall få innehålla. Med hänsyn till arten av de verksamheter vilka nu är i fråga är det emellertid enligt vår uppfattning inte möjligt att i detalj reglera i lag vilka uppgifter som bör få behandlas. En noggrann reglering av vilka uppgifter som bör få behandlas måste även till viss del vara hemlig.

Genom att det i lagförslagen noggrant anges för vilka ändamål personuppgifter får behandlas har en övergripande ram dragits upp för vilka kategorier av uppgifter som får behandlas. Den närmare regleringen av vilka kategorier av uppgifter som skall få behandlas bör återfinnas i förordning, regeringsbeslut eller, om regeringen bestämmer det, i myndighetsföreskrifter. I våra förslag till förordning för Forsvarsmakten respektive Forsvarets radioanstalt har vi tagit in bestämmelser som anger att vissa typer av uppgifter får behandlas. Vi överlåter emellertid till respektive myndighet att närmare bestämma vilka uppgifter som får behandlas i verksamheten.

Utan att uttryckligen i lagförslagen reglera vilka uppgifter som får behandlas i databaserna föreslår vi vissa begränsningar när det gäller den militära säkerhetstjänsten (se avsnitt 8.2.4). De föreslagna lagarna bör kunna ge en viss vägledning för vilka uppgifter som finns registrerade med hänsyn till arten av den verksamhet som beskrivs och till de ändamål för vilka personuppgifter får behandlas, såväl inom Forsvarsmaktens som inom Forsvarets radioanstalts verksamhet.

Att överhuvudtaget inte ha någon reglering av vilka uppgifter som får behandlas i myndigheternas databaser innebär att enskilda inte direkt skulle kunna utläsa vilka uppgifter om dem som eventuellt finns registrerade, och detta skulle av vissa kunna uppfattas som en brist i författningsregleringen. I den nu gällande förordningen (2001:703) om viss behandling av personuppgifter inom Forsvarsmakten och Forsvarets radioanstalt finns bestämmelser om vilka uppgifter ett försvarsunderrättelse- respektive säkerhetsregister får innehålla. I bestämmelserna anges bl.a. att registren får innehålla uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade är av betydelse för den aktuella verksamheten. En sådan bestämmelse

innebär i praktiken ingen begräsning av vilka uppgifter som får behandlas och fyller därmed ingen egentlig integritetsskyddande funktion. Vi har emellertid ändå stannat för att i våra förslag till förordningar om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet ta in motsvarande bestämmelser om innehåll när det gäller uppgifter i myndigheternas databaser. Av det ovan anförda framgår att det helt och hållet är verksamhetens krav och syftet med den aktuella behandlingen – inom den ram som bestämmelserna om tillåtna ändamål för behandlingen av personuppgifter medger – som får avgöra vilka uppgifter som får behandlas. Enligt vår uppfattning kan emellertid en bestämmelse om innehåll ändå ge en viss information till den enskilde om vilka uppgifter som får registreras och bör av upplysningsskäl finnas med i författningsregleringen. Vi föreslår därför att det i myndigheternas databaser får behandlas uppgifter som avser identifiering av enskilda, de omständigheter och händelser som ger anledning anta att den registrerade har betydelse för den aktuella verksamheten, upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet samt hänvisningar till de ärenden där uppgifter om den registrerade behandlas.

8.3.5 Begränsningar vid sökning i databaserna

Vårt förslag: Vid sökning i Försvarets radioanstalts databaser skall känsliga personuppgifter inte få användas som sökbegrepp om det inte är nödvändigt.

Vid sidan av innehållet i och åtkomsten till register och databaser är frågan om på vilket sätt uppgifter kan sammanställas en av de viktigare från integritetssynpunkt. Ju större möjligheter det finns att sammanställa uppgifter om enskilda, desto större blir riskerna för otillbörliga intrång i den personliga integriteten. Den metod som i dag främst används för att förhindra att det görs oönskade sammanställningar är begränsningar av sökmöjligheterna.

Det är framför allt i ett avseende som vi anser att det av integritetsskäl finns anledning att ha rättsliga begränsningar för vilka uppgifter som skall få användas vid sökning efter uppgifter i Försvarets radioanstalts databaser. Det gäller känsliga

personuppgifter, som får behandlas endast som ett komplement till de andra uppgifter som är skälet till att personen i fråga förekommer i databasen (se avsnitt 8.2.5). Enligt vår mening bör det inte vara möjligt att fritt söka efter information om känsliga personuppgifter i databaserna om det inte är nödvändigt för syftet med behandlingen. En uppgift om t.ex. etnisk härkomst får således användas som sökbegrepp bara under den förutsättningen att det är nödvändigt för att få fram den information som behövs för att t.ex. utföra en fredsbevarande eller humanitär insats som åligger svenskt förband eller annan organisationsenhet.

Redan av bestämmelsen om känsliga personuppgifter i 1 kap. i lagförslagen följer en begränsning av möjligheten att använda känsliga personuppgifter som sökord (se avsnitt 8.2.5). Syftet med att ta in en särskild paragraf om användningen av känsliga personuppgifter som sökord är att förtydliga vilka praktiska konsekvenser bestämmelsen i 1 kap. får. Det är inte nödvändigt att vid användning av en känslig personuppgift som sökord alltid använda ett kompletterande sökord som inte utgör en känslig personuppgift. Däremot får sökning inte ske enbart med den känsliga personuppgiften som grund utan måste ske av ett för verksamheten annat berättigat skäl. Avsikten med bestämmelserna är att känsliga personuppgifter inte skall användas i verksamheten utan att föregås av ett noggrant övervägande huruvida användningen av personuppgifterna tillför något av värde för verksamheten i övrigt. Endast under en sådan förutsättning får en känslig personuppgift användas vid sökning efter information i en av Försvarmaktens eller Försvarets radioanstalts databaser.

8.3.6 Direktåtkomst

Vårt förslag: Vilka som får ha direktåtkomst till Försvarmaktens informationsdatabas eller underrättelse- och säkerhetsdatabas bestäms av regeringen i förordning eller beslut.

I Försvarets radioanstalts underrättelseverksamhet får direktåtkomst förekomma endast till myndighetens rapportdatabas. Vilka som får ha direktåtkomst till rapportdatabasen bestäms av regeringen i förordning eller beslut.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten till databaser i Försvarmaktens försvars-

underrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Vad är direktåtkomst?

I många registerförfattningar och andra författningar som reglerar behandling av personuppgifter finns det bestämmelser där direktåtkomst till myndigheters register och databaser regleras särskilt. Med direktåtkomst avses vanligtvis att någon har direkt tillgång till ett register eller en databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. Normalt kan information som finns tillgänglig via direktåtkomst kopieras av mottagaren och därefter bearbetas av denne.

I begreppet direktåtkomst ligger också att den som är ansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av. Det innebär att den som har direktåtkomst till samtliga uppgifter i en myndighets register själv kan välja vilka uppgifter han eller hon vill ta del av vid ett visst tillfälle, utan att myndigheten först fattar ett beslut om att uppgifterna skall lämnas ut.

Direktåtkomst och sekretess

Möjligheterna att vid informationsutbyte mellan exempelvis två myndigheter utnyttja direktåtkomst, kan dock begränsas av sekretesslagens bestämmelser. En myndighet kan enligt vår mening inte tillåtas att få direktåtkomst till ett register eller en databas, om uppgifterna omfattas av sekretess som innebär att den mottagande myndigheten vid en prövning enligt sekretesslagen inte med säkerhet skulle ha rätt att ta del av uppgifterna. I och med att direktåtkomst innebär att den mottagande myndigheten fritt kan avgöra vilka uppgifter den vill ta del av, så måste uppgifterna nämligen enligt vår uppfattning anses utlämnade i och med att direktåtkomsten finns. Det spelar i det avseendet ingen roll om den mottagande myndigheten faktiskt använder sig av en viss uppgift eller inte.

En förutsättning för direktåtkomst torde därför vara att åtkomsten avser endast uppgifter för vilka det inte är föreskrivet sekretess *eller* uppgifter som enligt lag eller förordning skall lämnas ut till den som har direktåtkomst (se 14 kap. 1 § sekretesslagen)

eller uppgifter som, enligt prövning på förhand, med stöd av generalklausulen i 14 kap. 3 § sekretesslagen får lämnas ut rutinmässigt till den som har direktåtkomst. Det har emellertid i olika sammanhang diskuterats om bestämmelser om direktåtkomst generellt kan, eller bör, ges den innebörden att de bryter eventuell sekretess för de uppgifter till vilka det föreskrivs direktåtkomst (se t.ex. prop. 2001/01:33, s. 131 och 347f.).

Med hänsyn till att det råder osäkerhet i frågan om eller när bestämmelser om direktåtkomst skall tillmätas sekretessbrytande verkan, föreslår vi att det i författningarna om behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet endast anges att någon *får* ha direktåtkomst till en uppgift, inte att någon *skall* ha sådan åtkomst. Vår avsikt är att markera att bestämmelserna om direktåtkomst inte har sekretessbrytande verkan. Direktåtkomst som tillåts enligt de av oss föreslagna lagarna torde därmed i praktiken kunna medges endast i två fall, nämligen om de aktuella uppgifterna är offentliga, dvs. att det inte är föreskrivet om sekretess för dem, eller om det finns en skyldighet enligt sekretesslagen eller annan lag eller förordning att lämna ut de aktuella uppgifterna till den som får ha direktåtkomst.

Direktåtkomst till databaser hos Försvarmakten och Försvarets radioanstalt

Vid bedömningen av vilka som bör få ha direktåtkomst till en databas i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet bör utgångspunkten vara att sådan åtkomst kan tillåtas, men att det inte skall ske i större omfattning än vad som kan försvaras av effektivitetsskäl. Det är enligt vår mening viktigt att en principiell avvägning görs mellan hänsynen till å ena sidan myndigheternas effektivitet och å andra sidan de registrerades integritet.

En grundläggande utgångspunkt måste enligt vår mening vara att direktåtkomst endast bör tillåtas när nyttan av åtkomsten är klart påvisbar samtidigt som den inte innebär några beaktansvärda försämringar av skyddet för enskildas integritet. Samtidigt bör i detta sammanhang beaktas vad vi på flera ställen framhåller vad avser den sekretess och säkerhet i övrigt som gäller inom de

aktuella verksamheterna. Det är av grundläggande betydelse för såväl Försvarmakten som Försvarets radioanstalt att myndigheternas information inom såväl försvarsunderrättelseverksamheten som säkerhetstjänsten inte sprids till obehöriga. Av detta följer att det ligger i myndigheternas eget intresse att inte tillåta direktåtkomst utan att dessa omständigheter beaktas fullt ut.

Som tidigare framgått är det för såväl försvarsunderrättelseverksamhet som militär säkerhetstjänst av stor vikt att ha ett brett samarbete med andra myndigheter. Regeringen har påtalat detta i regleringsbrev för såväl Försvarmakten som Försvarets radioanstalt. Ett viktigt medel i detta samarbete är naturligtvis utbyte av information. För att kunna uppnå en hög effektivitet i informationsutbytet anser vi att det är nödvändigt att utnyttja de bästa tekniska hjälpmedel som finns i dag. Stor betydelse i detta sammanhang har givetvis möjligheten till direktåtkomst till viktiga databaser.

Direktåtkomst förekommer i dag när det gäller vissa av Försvarmaktens databaser. Till den militära underrättelse- och säkerhetstjänstens Informationsdatabas har Försvarets materielverk, Försvarets radioanstalt och Regeringskansliet direktåtkomst. Uppgifterna i IS UNDSÅK är tillgängliga genom direktåtkomst för Regeringskansliet, Försvarets materielverk, Försvarets radioanstalt, Tullverket, Krisberedskapsmyndigheten och inom kort även för Totalförsvarets forskningsinstitut. Någon reglering av denna direktåtkomst finns dock inte, vilket är otillfredsställande. Enligt vår uppfattning bör det i lag eller förordning eller i särskilda regeringsbeslut framgå att direktåtkomst förekommer.

Fråga är då hur direktåtkomst bör regleras när det gäller Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet. I andra registerförfattningar anges vanligen i lag vilka myndigheter som får ha direktåtkomst, medan det överläts till regeringen att närmare bestämma omfattningen av sådan direktåtkomst. Enligt vår uppfattning är en sådan reglering emellertid inte i sin helhet lämplig för Försvarmakten och Försvarets radioanstalt, särskilt vad gäller försvarsunderrättelseverksamhet.

Som tidigare framhållits lämpar sig försvarsunderrättelseverksamhet dåligt för att närmare regleras i lag. Det är regeringen som bestämmer vilka myndigheter som skall bedriva försvarsunderrättelseverksamhet och som i regleringsbrev och andra beslut bestämmer verksamhetens inriktning. Försvarsunderrättelse-

verksamhet styrs av regeringen även genom mer informella kontakter och den fortlöpande uppföljningen av verksamheten sker av Samordningssekretariatet för säkerhetspolitiska underrättelsefrågor i Regeringskansliet (SUND), jfr. avsnitt 2.4. Vidare gäller att det med mycket kort varsel kan behöva ske förändringar av vem som bör få ha direktåtkomst till databaserna. Det är då olämpligt om sådan anpassning inte kan ske inom rimlig tid därför att en ändring kräver lagform. Mot bakgrund härav talar enligt vår uppfattning övervägande skäl för att det är regeringen som, genom förordning eller särskilt beslut, bör bestämma vilka myndigheter som får ha direktåtkomst till aktuella databaser hos Försvarmakten och Försvarets radioanstalt.

Vi föreslår därför att det i lag anges att regeringen får bestämma vem som får ha direktåtkomst till databaser i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. När det gäller omfattningen av direktåtkomsten bör detta beslutas av regeringen eller av den myndighet regeringen bestämmer. I våra förslag till förordning för respektive myndighet har vi angivit vilka myndigheter som får ha direktåtkomst och till vilka databaser. Där anges också att det är Försvarmakten respektive Försvarets radioanstalt som bestämmer omfattningen av den direktåtkomst som får förekomma.

I dag förekommer ingen direktåtkomst till någon av Försvarets radioanstalts databaser. Enligt vår uppfattning är det av integritetsskäl främst myndighetens rapportdatabas som kan komma i fråga när det gäller direktåtkomst. I rapportdatabasen finns de färdiga underrättelserapporter som skall delges myndighetens uppdragsgivare. I andra databaser hos Försvarets radioanstalt kan det finnas obearbetat signalspaningsmaterial som kan innehålla känsliga personuppgifter. Direktåtkomst bör därför enligt vår mening få förekomma endast till rapportdatabasen.

Naturligtvis kan det finnas skäl att lämna ut information även från andra databaser än rapportdatabasen på automatiserad väg på annat sätt än genom direktåtkomst. Det kan då t.ex. ske genom att en fil avskiljs och görs tillgänglig för en myndighet eller genom att en cd-romskiva översänds till en uppdragsgivare. Ett utlämnande av information från andra databaser än rapportdatabasen bör emellertid ske först efter vederbörlig sekretessprövning och inte genom att mottagande myndighet genom direktåtkomst ges möjlighet att själv gå in och välja information (jfr. avsnitt 9.2.2). Däremot kan det som nämnts inte anses föreligga hinder mot att en

uppdragsgivare ges möjlighet att genom direktåtkomst på egen hand gå in i rapportdatabasen och läsa sina beställda rapporter, vilka annars skulle tillställas denne i annan form.

8.4 Enskildas rättigheter

Dataskyddsdirektivets regler om enskildas rättigheter i samband med behandling av personuppgifter är av central betydelse för skyddet av de registrerades personliga integritet. För att otillbörligt intrång i den personliga integriteten i största möjliga mån skall undvikas har det ansetts nödvändigt att enskilda tillskrivs särskilda rättigheter. Mot bakgrund härav finns i personuppgiftslagen bestämmelser om bl.a. information, rättelse och skadestånd. Att enskilda ges möjlighet till insyn i vad som finns registrerat om dem i olika databaser och register är av betydelse för att de skall kunna kräva rättelse av felaktiga uppgifter. När personuppgiftsansvariga behandlar uppgifter i strid med gällande regler, har det ansetts att de enskilda skall kunna få ersättning för skada och kränkning av den personliga integriteten.

Inom de särskilda registerförfattningarnas områden har det av rättssäkerhetsskäl vidare ansetts viktigt att myndigheternas beslut i frågor som rör rätten till information och krav på att behandlade uppgifter är korrekta, kan överklagas av enskilda i den för förvaltningsbeslut gällande ordningen.

Till skillnad från de bestämmelser som avser databaser, är de särskilda bestämmelser om enskildas rättigheter som redovisas i detta kapitel endast tillämpliga på behandling av personuppgifter. Det är med andra ord endast fysiska personer som är i livet (jfr. 3 § personuppgiftslagen) som över huvud taget kan kräva information om utförd behandling eller rättelse av felaktiga uppgifter. Det är vidare bara fysiska personer som kan överklaga myndigheternas beslut i sådana frågor och som med stöd av den lagstiftning vi föreslår kan kräva skadestånd av den personuppgiftsansvariga myndigheten.

8.4.1 Information

Vårt förslag: Personuppgiftslagens bestämmelser om information som skall lämnas självant till den registrerade när uppgifter har samlats in från honom själv och om information som skall lämnas efter ansökan av den registrerade, skall i huvudsak tillämpas vid behandling av personuppgifter inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Innehållet i personuppgiftslagens bestämmelser om information till den registrerade redogör vi kortfattat för i avsnitt 4.7.4.

Av 23 § personuppgiftslagen framgår att den personuppgiftsansvarige självant skall informera en enskild om behandling av uppgifter som samlas in från den enskilde själv. Den information som skall lämnas är uppgifter om den personuppgiftsansvariges identitet, ändamålen med behandlingen samt övrig information som behövs för att den registrerade skall kunna ta tillvara sina rättigheter. Bestämmelsen har sin grund i artikel 10 i dataskyddsdirektivet. Vi anser att bestämmelsen bör vara tillämplig på behandling av personuppgifter inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Annorlunda är det med 24 § personuppgiftslagen. Där anges det i enlighet med artikel 11 i dataskyddsdirektivet att den registrerade skall informeras även när uppgifter har samlats in från någon annan källa än honom själv. Sådan information behöver nämligen inte lämnas om det finns bestämmelser om registreringen i lag eller annan författning. När behandling av personuppgifter hos en myndighet regleras i särskild lagstiftning på det sätt som vi föreslår för Försvarmakten och Försvarets radioanstalt, med bestämmelser om vad som får registreras och hur uppgifter i övrigt får hanteras, krävs det enligt personuppgiftslagen således inte att sådan information ges. Vi har inte funnit några skäl för att Försvarmakten och Försvarets radioanstalt trots detta skall lämna sådan information. Bestämmelsen i 24 § personuppgiftslagen bör således inte tillämpas på behandling enligt den av oss föreslagna lagstiftningen.

Den från integritetssynpunkt kanske viktigaste bestämmelsen i dataskyddsdirektivet återfinns i artikel 12 a). Enligt denna har

enskilda rätt att få information av den personuppgiftsansvarige om personuppgifter som rör den registrerade behandlas eller inte. Om uppgifter behandlas skall information lämnas om vilka uppgifter det rör sig om, varifrån uppgifterna har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna har lämnats ut. Bestämmelsen har sin motsvarighet i 26 § personuppgiftslagen, där enskilda garanteras denna rätt till information efter ansökan. Information behöver emellertid inte lämnas beträffande personuppgifter som behandlas endast i löpande text som ännu inte fått sin slutliga utformning eller som utgör minnesanteckningar, under förutsättning att uppgifterna inte har lämnats ut till tredje man. Bestämmelsen i personuppgiftslagen bör vara tillämplig vid behandling av personuppgifter enligt den av oss föreslagna lagstiftningen.

Även 27 § personuppgiftslagen anser vi skall vara tillämplig på behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Det innebär att om det i lag eller annan författning, eller i beslut som har meddelats med stöd av författning, särskilt har föreskrivits att uppgifter inte får lämnas ut till den registrerade, så gäller inte de ovan redovisade bestämmelserna i personuppgiftslagen om information. Enligt vår uppfattning medför detta speciella konsekvenser när det gäller skyddet för den personliga integriteten vid behandling av personuppgifter inom de verksamheter som våra författningsförslag omfattar. Våra överväganden i detta sammanhang redovisas i avsnitt 8.5 om särskild granskning till skydd för den personliga integriteten.

8.4.2 Rättelse och skadestånd

Vårt förslag: Personuppgiftslagens bestämmelser om rättelse av personuppgifter och om skadestånd skall tillämpas vid behandling av personuppgifter inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Personuppgiftslagens bestämmelser om rättelse

I korthet innebär bestämmelsen om rättelse i 28 § personuppgiftslagen att den personuppgiftsansvarige är skyldig att på begäran av den registrerade rätta, blockera eller utplåna sådana personuppgifter som inte behandlats i enlighet med lagstiftningen. Den personuppgiftsansvarige har även, med vissa undantag, en skyldighet att underrätta tredje man till vilken uppgifterna lämnats ut om korrigeringsåtgärden.

Redan av de grundläggande kraven i 9 § personuppgiftslagen framgår emellertid att den personuppgiftsansvarige på egen hand måste vara aktiv för att se till att de behandlade uppgifterna är korrekta. Bestämmelsen i 28 § personuppgiftslagen innehåller således regler om en rätt för den registrerade att påkalla den personuppgiftsansvariges aktivitet för att korrigera uppgifter, som gäller utöver de grundläggande kraven på den personuppgiftsansvarige enligt 9 § (jfr. Öman m.fl., Personuppgiftslagen En kommentar, 2:uppl. s. 217).

Att en personuppgift rättas innebär att den ersätts eller kompletteras med korrekta uppgifter. Med blockering avses en åtgärd som vidtas för att personuppgifter skall vara förknippade med information om att de är spärrade och om anledningen till spärren. Att en uppgift utplånas innebär att den förstörs så att den inte kan återskapas. Skyldigheten att vidta rättelse åligger den personuppgiftsansvarige.

Det är enligt vår uppfattning av väsentlig betydelse att personuppgifter som behandlas felaktigt hos en myndighet rättas för att intrång i den personliga integriteten skall undvikas. Bedömningen av om en uppgift har behandlats felaktigt måste göras mot bakgrund av de bestämmelser som gäller för behandlingen, oavsett om det är grundläggande regler i personuppgiftslagen eller specialbestämmelser som gäller för Försvarmakten och Försvarets radioanstalt. Vi föreslår därför att bestämmelsen om rättelse i 28 § personuppgiftslagen skall tillämpas vid behandling av personuppgifter enligt de av oss föreslagna författningarna.

När skall rättelse vidtas?

En personuppgift skall rättas när den har behandlats felaktigt. I princip är all behandling av personuppgifter felaktig som strider mot den lagstiftning som reglerar behandlingen. Att i detalj ange

vad som är felaktig behandling är därför inte möjligt, men något förenklat anser vi att en indelning av olika fel kan göras i två grupper. Felaktig behandling kan för det första bestå i att personuppgifter är oriktiga till sitt innehåll, dvs. felet finns inbyggt i uppgifterna (oriktiga uppgifter). Felaktig behandling kan även bestå i att personuppgifter, oavsett om de är korrekta eller inte, används på ett felaktigt sätt i verksamheten, dvs. felet ligger i hur uppgifterna används (oriktig användning). Bedömningen av om en uppgift används på ett oriktigt sätt måste göras mot bakgrund av de bestämmelser som gäller för behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Oriktig användning kan t.ex. innebära att en uppgift används på ett sätt som är oförenligt med de ändamål som gäller för verksamheten.

Det är emellertid inte alltid självklart om en uppgift är oriktig. Det viktiga i det här sammanhanget är enligt vår uppfattning att bedömningen av om en uppgift skall anses vara oriktig eller inte, dvs. om den skall rättas, görs mot bakgrund av vilka krav verksamheten ställer på uppgiftsbehandlingen. Även om det inte är möjligt att ge en exakt definition på vad som är en oriktig uppgift, anser vi att man bör ha följande utgångspunkt. En uppgift är, trots att den inte återger en korrekt bild av ett sakförhållande, inte oriktig i den bemärkelsen att den måste rättas, om den korrekt återger ett händelseförlopp i verksamheten och dessutom behövs i densamma.

Enskildas rätt till skadestånd

Enligt 48 § personuppgiftslagen skall den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med lagen har orsakat. Skadestånd kan komma i fråga vid varje brott mot lagen och utgår trots att ingen har skadats fysiskt eller ekonomiskt och trots att den personuppgiftsansvarige inte haft uppsåt att göra fel eller varit försumlig vid behandlingen. Bakgrunden till denna stränga reglering är att bestämmelsen om skadestånd, precis som enskildas rättigheter i övrigt enligt lagen, rätt till information och rättelse m.m., har till syfte att skydda människor mot kränkning av den personliga integriteten genom behandling av personuppgifter (jfr. prop. 1997/98:44 s. 106, SOU 1997:39 s. 432).

Rätt till skadestånd bör finnas även för skada och kränkning som uppstår när uppgifter behandlas i strid med de särskilda bestämmelserna i våra lagförslag. Vi föreslår därför att bestämmelserna om skadestånd i 48 § personuppgiftslagen skall tillämpas när personuppgifter behandlas i strid med den av oss föreslagna lagstiftningen.

I likhet med vad som gäller de rättsliga möjligheterna att få information eller att få uppgifter rättade, gäller rätten till skadestånd endast levande fysiska personer. En juridisk person får i stället i den ordning som gäller för statlig verksamhet i allmänhet vända sig till justitiekanslern om den juridiska personen anser att behandling av uppgifter inom Försvarmakten eller Försvarets radioanstalt har vållat skada.

8.4.3 Överklagande

Vårt förslag: Försvarmaktens och Försvarets radioanstalts beslut om rättelse och om information som skall lämnas efter ansökan av en registrerad skall kunna överklagas.

Överklagande skall ske till allmän förvaltningsdomstol, dvs. länsrätt. Prövningstillstånd skall krävas vid överklagande till kammarrätt.

Beslut av en myndighet som direkt berör en enskild och som inte är av rent intern administrativ karaktär, bör enligt vår uppfattning i allmänhet kunna överklagas. I fråga om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet gäller det framför allt beslut att avslå en ansökan om information om pågående behandlingar samt beslut att avslå en begäran om rättelse. Överklagande bör enligt vår uppfattning vara möjligt i båda fallen.

Den normala ordningen när en myndighet fattar beslut av förvaltningskaraktär är enligt 22 a § förvaltningslagen (1986:223) att beslutet kan överklagas hos allmän förvaltningsdomstol (länsrätt) och att det krävs prövningstillstånd för vidare överklagande till kammarrätten. Detta är också vad som generellt gäller för nyare författningar om behandling av personuppgifter i offentlig verksamhet (jfr. SFS 2001:85, 181–185, 454 och 935).

8.5 Särskild granskning till skydd för den personliga integriteten

Vårt förslag: Till skydd för den personliga integriteten bör Försvarets underrättelsenämnd få i uppdrag att särskilt granska den behandling av personuppgifter som sker inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Som en följd härav föreslår vi att Försvarets underrättelsenämnds ansvarsområde utökas till att omfatta även den militära säkerhetstjänsten.

Av artikel 13 i dataskyddsdirektivet framgår att undantag från informationsbestämmelserna och bestämmelserna om rättelse m.m. får göras då det är nödvändigt med hänsyn till t.ex. statens säkerhet och försvaret samt skydd av den registrerades eller andras fri- och rättigheter. Sverige har med stöd härav i 27 § personuppgiftslagen gjort undantag från informationsskyldigheten enligt 23-26 §§ samma lag vid sekretess och tystnadsplikt. Undantaget innebär att sekretess och tystnadsplikt alltid går före den i personuppgiftslagen föreskrivna informationsskyldigheten.

För uppgifter som behandlas i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet gäller sekretess av olika skäl och av olika grad. Enligt 2 kap. 1 § sekretesslagen gäller sekretess för uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Enligt 2 § samma kapitel gäller sekretess för uppgift som angår verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

Som angivits tidigare är det vår uppfattning att undantaget från informationsskyldighet vid sekretess och tystnadsplikt enligt 27 § personuppgiftslagen skall gälla för Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet. Detta framstår

som helt självklart. Med hänsyn till arten av den verksamhet som bedrivs är det helt nödvändigt att den är förenad med sekretess och det skulle vara synnerligen olämpligt om enskilda skulle kunna få en sådan insyn i den hemliga verksamheten som en informations-skyldighet enligt personuppgiftslagen innebär.

Till skillnad från andra myndigheters behandling av personuppgifter, där samma undantag från informationsskyldigheten gäller, får emellertid i detta sammanhang undantaget alldeles särskilda konsekvenser när det gäller de enskildas rättigheter och deras funktion som skydd för den personliga integriteten.

Personuppgiftslagens regler om enskildas rätt till information hör till de viktigaste medlen enligt den lagstiftningen för att personuppgifter inte skall behandlas på ett sätt som kan medföra att enskildas personliga integritet kränks. Den sekretess som gäller för uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet innebär emellertid att någon information i den mening som avses i personuppgiftslagen i praktiken aldrig kommer att lämnas av den personuppgiftsansvariga myndigheten. Till skydd för verksamheten gäller i underrättelseverksamheten och säkerhetstjänsten sekretess för i stort sett varje uppgift. Många uppgifter är hemliga såväl med hänsyn till Sveriges förhållande till främmande makt som till skydd för rikets säkerhet. Det är också viktigt att skydda uppgiftslämnare och arbetsmetoder. Detta får till följd att en begäran om information enligt personuppgiftslagens regler i det närmaste undantagslöst kommer att avslås med hänvisning till att sekretess gäller för uppgifterna. Utan kunskap om vilka uppgifter som behandlas kommer den enskilde inte att kunna utnyttja möjligheten att begära rättelse eller i övrigt kontrollera att uppgifter om honom eller henne behandlas korrekt och i enlighet med vad som är särskilt föreskrivet.

Personuppgiftslagens regler om information och rättelse m.m. kan alltså fylla en viktig funktion i de få sammanhang där sekretess inte råder för uppgifterna, och det är enligt vår uppfattning viktigt att dessa regler är tillämpliga. Mot bakgrund av vad som ovan angivits är det emellertid enligt vår uppfattning nödvändigt att de registrerades personliga integritet dessutom värnas på något annat sätt vid Försvarmaktens och Försvarets radioanstalts behandling av personuppgifter. Som ett komplement till bestämmelserna om information måste därför andra åtgärder vidtas för att åstadkomma ett rimligt skydd för den personliga integriteten.

Hänsyn till sekretessen inom försvarsunderrättelseverksamhet och militär säkerhetstjänst framstår i detta sammanhang som helt avgörande. Underrättelseutredningen uttalade i betänkandet Den militära underrättelsetjänsten (SOU 1976:129) följande i samband med sitt förslag att inrätta Försvarets underrättelsenämnd. En djup sekretess är nödvändig kring stora delar av det militära underrättelseväsendet av hänsyn till landets säkerhet och förhållandet till främmande makter. Enskilda medborgare har därför små möjligheter att själva informera sig om underrättelsetjänsten och bilda sig en uppfattning i frågor som rör denna. Under sådana förhållanden är det betydelsefullt att begränsningarna i den enskilda insynen uppvägs av en effektivt verkande kontroll genom statsmakternas försorg (jfr. SOU 1976:19 s. 129).

I detta sammanhang bör nämnas att inom polisens område har Registernämnden fått till särskild uppgift att värna skyddet för den personliga integriteten (jfr. avsnitt 2.6.1). Nämnden skall i första hand pröva frågor om utlämnande av uppgifter från vissa av polisens register i samband med registerkontroll. Registernämnden har emellertid därutöver också till uppgift att granska Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen, särskilt med avseende på behandlingen av känsliga personuppgifter. I anknytning härtill vill vi även peka på vad Svea hovrätt framhållit i remissyttrande (2002-09-20, Dnr 316/02) över Polisdatautredningens förslag till ny polisdatalag (SOU 2001:92). Hovrätten framhåller i yttrandet att krav måste ställas på en kontinuerlig och effektiv tillsyn över registerföringen. Domstolen anser att Polisdatautredningens förslag väcker frågan om inte motsvarande granskning som Registernämnden utövar när det gäller Säkerhetspolisens behandling av uppgifter enligt polisdatalagen borde övervägas även för den öppna polisen.

Enligt vår uppfattning bör även den aktuella behandlingen av personuppgifter hos Försvarsmakten och Försvarets radioanstalt underkastas en särskild granskning genom statsmakternas försorg.

8.5.1 Försvarets underrättelsenämnd

Försvarets underrättelsenämnd inrättades den 1 juli 1976. Syftet med en underrättelsenämnd var att denna skulle utgöra regeringens insyns- och kontrollorgan med uppgift att fortlöpande följa verksamheten hos den militära underrättelsetjänsten och att lämna de förslag som föranleddes av granskningen.

Enligt 1 § förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd har Försvarets underrättelsenämnd till uppgift att följa underrättelsetjänsten inom Försvarmakten och de övriga myndigheter som enligt förordningen (2000:131) om försvarsunderrättelseverksamhet bedriver försvarsunderrättelseverksamhet, såsom Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut.

Försvarets underrättelsenämnd skall enligt 2 § i sin instruktion särskilt

- följa hur lagen (2000:130) och förordningen (2000:131) om försvarsunderrättelseverksamhet tillämpas,
- granska att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning som är bestämd,
- ägna uppmärksamhet åt de enheter inom Försvarmakten och Försvarets radioanstalt som inhämtar underrättelser med särskilda metoder,
- granska de medel och metoder för inhämtning av underrättelser som används,
- granska hur de register som behövs för försvarsunderrättelseverksamheten läggs upp och förs, samt
- granska principer för rekrytering och utbildning av personal.

Försvarets underrättelsenämnd skall lämna Försvarmakten och de övriga myndigheter som bedriver försvarsunderrättelseverksamhet de synpunkter och de förslag till åtgärder som föranleds av granskningsverksamheten. Om det behövs skall nämnden också lämna förslag om åtgärder till regeringen. Försvarets underrättelsenämnd skall senast den 1 mars varje år till regeringen lämna en rapport över föregående års granskningsverksamhet.

Försvarets underrättelsenämnd består av sex ledamöter, varav en är ordförande, som utses av regeringen för en bestämd tid.

Försvarets underrättelsenämnds kontroll innebär i första hand att följa hur lagen och förordningen om försvarsunderrättelseverksamhet tillämpas i verksamheten. Nämnden granskar också att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning som är bestämd och ägnar särskild uppmärksamhet åt de enheter inom Försvarmakten och Försvarets radioanstalt som inhämtar underrättelser med särskilda metoder. Försvarets underrättelsenämnd granskar även de medel och metoder för inhämtning av underrättelser som används, hur de register och databaser som behövs för försvarsunderrättelseverksamheten läggs upp och förs samt granskar principer för rekrytering och utbildning av personal.

8.5.2 Vårt förslag om särskild granskning

Försvarets underrättelsenämnd har till uppgift att följa underrättelsetjänsten inom Försvarmakten och de övriga myndigheter som bedriver försvarsunderrättelseverksamhet, bl.a. Försvarets radioanstalt. Nämnden kontrollerar att underrättelseverksamheten bedrivs i enlighet med gällande riktlinjer och kontrollerar de medel och metoder som används för inhämtning av underrättelser. Härvid har nämnden som särskild uppgift att granska hur de register som behövs för försvarsunderrättelseverksamheten läggs upp och förs. Försvarets underrättelsenämnd har vana att iakta den sekretess som gäller för uppgifter i underrättelsetjänsten och nämnden framstår även med hänsyn till kunskaperna om försvarsunderrättelseverksamhet och från säkerhetsskyddssynpunkt som bäst lämpad att utföra granskning av behandlingen av personuppgifter. Vi föreslår därför att nämndens uppdrag utökas till att även omfatta granskning av behandlingen av personuppgifter enligt de författningar vi nu föreslår. Alternativet till Försvarets underrättelsenämnd som särskilt granskningsorgan är enligt vår uppfattning att inrätta ett helt nytt organ som får denna uppgift, i likhet med Registernämnden inom polisens område.

För Försvarets underrättelsenämnd gäller att den enligt 1 § förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd har till uppgift att följa underrättelsetjänsten inom Försvarmakten och de övriga myndigheter som bedriver försvarsunderrättelseverksamhet. Försvarets underrättelsenämnd har emellertid, enligt särskilt regeringsuppdrag, även granskat den militära säkerhetstjänsten (jfr. SOU 2002:87 s. 73). För att Försvarets underrättelsenämnd skall kunna utföra uppgiften att granska verksamheten med avseende på behandling av personuppgifter – inom såväl underrättelse- som säkerhetstjänst – bör nämndens uppgifter enligt instruktionen utvidgas till att även omfatta säkerhetstjänsten. Vi föreslår således att det i 1 § förordningen (1998:552) med instruktion för Försvarets underrättelsenämnd görs ett tillägg av innebörd att nämnden även har att följa den militära säkerhetstjänsten. Ett sådant tillägg medför att även nämndens traditionella granskning kommer att avse den militära säkerhetstjänsten. Härigenom kommer den granskning nämnden redan i dag utför av den militära säkerhetstjänsten, och som närmast oundvikligen följer av att verksamheten är så nära integrerad med underrättelsetjänsten, att uttryckligen ingå i nämndens uppgifter.

Viktigt att framhålla i detta sammanhang är att vårt förslag om en särskild granskning av Försvarets underrättelsenämnd inte på något sätt syftar till att inskränka det övergripande tillsynsansvar som åligger Datainspektionen enligt personuppgiftslagen. Inom Säkerhetspolisens område har Registernämnden som särskild uppgift att granska behandlingen av uppgifter enligt polisdatalagen (1988:622), vilket dock inte förtar Datainspektionens tillsynsansvar över behandlingar av uppgifter enligt polisdatalagen. Enligt våra författningsförslag ges Datainspektionen också motsvarande befogenheter som tillsynsmyndighet över Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet som myndigheten har enligt personuppgiftslagen. Datainspektionen har således alltjämt huvudansvaret för tillsynen över behandlingen av personuppgifter hos Försvarsmakten och Försvarets radioanstalt. Den uppgift vi ger Försvarets underrättelsenämnd att granska myndigheterna skall utgöra en kompensation för att enskilda, på grund av den sekretess som gäller i verksamheten, inte kan utnyttja den möjlighet till skydd för den personliga integriteten som personuppgiftslagens regler om information och rättelse m.m. innebär. Nämndens granskning är en extra integritetsskyddskontroll som, utöver Datainspektionens tillsyn, syftar till att skydda de registrerade mot att deras personliga integritet kränks genom behandling av personuppgifter.

Med hänsyn till jämförelsen med Registernämnden kan det finnas anledning att framhålla att det inte är vår avsikt att Försvarets underrättelsenämnd skall vara involverad i någon löpande ärendehantering hos de båda myndigheterna eller att enskilda skall kunna vända sig till nämnden med begäran om utlämnande av handlingar. En sådan begäran skall som i dag prövas av Försvarsmakten eller Försvarets radioanstalt. Det ankommer på Försvarets underrättelsenämnd att i enlighet med vad som annars gäller för självständiga tillsynsorgan, själv bestämma de närmare formerna för hur granskningen lämpligast skall genomföras.

9 Särskilda frågor

9.1 Bevarande och gallring

Vårt förslag: Personuppgifter som behandlas i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet skall bevaras och gallras enligt reglerna i personuppgiftslagen (1998:204) och arkivlagen (1990:782).

Vi konstaterar tidigare att det uppstår integritetsproblem när stora mängder uppgifter om enskilda personer samlas hos myndigheter, i synnerhet som dagens teknik tillåter att avancerade sammanställningar av information kan göras på ett enkelt sätt (se avsnitt 7.2). En metod att minska integritetskänsligheten är att se till att uppgifter som inte längre behövs för en myndighets verksamhet avlägsnas från myndighetens databaser eller register. För att uppnå detta krävs bestämmelser om gallring av uppgifter eller om överlämnande av uppgifter till en arkivmyndighet. Vid utformningen av gallringsbestämmelser måste det dock hållas i minnet att offentlighetsprincipen, för att den inte skall bli verkningslös, ställer krav på att vissa uppgifter bevaras för framtiden. Uppgifter får i princip aldrig gallras i sådan omfattning att det äventyrar arkivens roll som en del av kulturarvet eller något av de tre huvudändamålen med arkivverksamheten. Även efter en genomförd gallring måste arkiven kunna tillgodose rätten att ta del av allmänna handlingar, rättskipningens och förvaltningens behov samt forskningens behov. Det går alltså inte att bara ange att samtliga uppgifter skall gallras när de inte behövs för verksamheten. Tvärtom behövs en avvägning mellan integritets- och offentlighetsintresset. Detta är viktigt inte minst i en tid då mängder av uppgifter finns endast i elektronisk form. En fullständig gallring av samtliga uppgifter i ett

dataregister kan omöjliggöra en senare rekonstruktion av händelseförlopp.

Grundläggande bestämmelser om bevarande och gallring av uppgifter hos myndigheter finns i 2 kap. tryckfrihetsförordningen och arkivlagen (1990:782). Enligt 3 § arkivlagen skall myndigheters arkiv bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättsskipningen och förvaltningen samt forskningens behov. Allmänna handlingar får enligt 10 § samma lag gallras endast om återstående arkivmaterial kan tillgodose dessa ändamål, och det krävs särskilda föreskrifter eller beslut av arkivmyndigheten för att gallring skall få ske. Hur länge personuppgifter får bevaras regleras dessutom i personuppgiftslagen som ett grundläggande krav på behandling av personuppgifter. I 9 § första stycket i) personuppgiftslagen anges nämligen att den personuppgiftsansvarige skall se till att personuppgifter inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det föreligger således en skyldighet enligt personuppgiftslagen att gallra personuppgifter som inte längre är nödvändiga med hänsyn till ändamålen med behandlingen. I fråga om personuppgifter som utgör allmänna handlingar och som behandlas i myndighetsverksamhet tillämpas dock i första hand bestämmelserna i arkivlagen, jfr. 8 § personuppgiftslagen. I de registerförfattningar som i dag gäller för statlig verksamhet finns regelmässigt även särskilda gallringsbestämmelser för uppgifter som behandlas automatiserat.

Vi har för vår del övervägt två alternativ till hur gallrings- och bevarandefrågor bör regleras i speciallagstiftningen för behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Det ena alternativet är att inte ha några särbestämmelser över huvud taget, vilket innebär att personuppgiftslagens och arkivlagens regler gäller fullt ut. Det andra alternativet är att i lag ange att samtliga uppgifter skall gallras och när det skall göras, men ge regeringen eller Riksarkivet möjlighet att besluta om undantag.

Det senare alternativet är det vanligaste i nya registerförfattningar och metoden utgår från att det i lag ställs upp huvudregler för när gallring skall ske. Regeringen eller Riksarkivet kan sedan besluta eller meddela föreskrifter om att uppgifter skall bevaras. Fördelen härmed har främst ansetts vara att särskild reglering behöver göras endast när det finns skäl för det. Vidare finns det direkt i lagtexten en "säkerhetsventil" mot att stora

uppgiftssamlingar med känsliga uppgifter bevaras, trots att de inte har något faktiskt värde för verksamheten, men på grund av sin omfattning kan vara skadliga från integritetssynpunkt. Eftersom metoden i princip innebär att allt skall gallras om inte regeringen eller Riksarkivet utfärdar föreskrifter om undantag, så ställs det krav på att regeringen eller Riksarkivet efter hand tar ställning till hur nya typer av uppgifter skall hanteras. Uppgifter och handlingar kan annars komma att gallras helt, vilket innebär att inte något material bevaras för framtiden. Riksarkivet har också kritiserat denna metod främst med motiveringen att lagstiftning med gallring som huvudregel tenderar att urholka offentlighetsprincipen och att Riksarkivet inte har praktisk möjlighet att ingripa med undantagsföreskrifter med hänsyn till det stora antalet registerlagar (se t.ex. SOU 2002:113 s. 339ff.).

Att inte ha några särbestämmelser över huvud taget, vilket innebär att arkivlagens regler är giltiga fullt ut, är den metod som tillämpas vad gäller traditionella pappersbaserade uppgifter i allmänna handlingar. Det finns starka skäl som talar för att samma förfarande bör gälla som huvudregel även i fråga om uppgifter som behandlas automatiserat, inte minst eftersom det blir allt vanligare att elektronisk information helt ersätter vanlig pappersbaserad information. Att generellt tillämpa den metoden innebär i och för sig att lagstiftaren inte har någon direkt kontroll över gallringsförfarandet vad avser de aktuella uppgifterna, utan de generella och allmänna bestämmelserna i arkivlagen gäller fullt ut. Tekniken har emellertid använts i annan lagstiftning som rör känsliga uppgifter. I lagen (1998:543) om hälsodataregister saknas bestämmelser om gallring, vilket innebär att arkivlagens bestämmelser blir tillämpliga. Regeringen konstaterade i förarbetena att en alltför omfattande gallring kunde leda till att det inte finns tillräckligt med material för t.ex. epidemiologiska undersökningar, medan en alltför begränsad gallring kunde leda till att känsliga uppgifter om enskilda sparas i onödan. På grund av svårigheterna med att i lagform reglera flera olika register som förändras över tiden avseende innehåll m.m., valde regeringen att låta arkivlagens bestämmelser gälla (prop. 1997/98:108 s. 59 f.).

Som tidigare framhållits krävs vid avgörande av vilken metod som skall gälla för bevarande och gallring en avvägning mellan integritets- och offentlighetsintresset. Gallring som huvudregel bör inte gälla utan att starkt vägande integritetsskäl talar härför. Enligt vår bedömning saknas det vid en sådan avvägning bärande skäl för att föreslå särskilda gallringsbestämmelser när det gäller

behandlingen av personuppgifter inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. De aktuella verksamheterna skiljer sig i stor utsträckning från vad som annars gäller i offentlig verksamhet. Vad som i detta sammanhang kanske är tydligast är det faktum att uppgifter med hänsyn till verksamheternas ändamål måste sparas under mycket lång tid. Detta gäller oavsett om uppgifterna behandlas i någon av myndigheternas databaser eller på annat sätt. I försvarsunderrättelseverksamhet är det inte ovanligt att uppgifter som är så gamla som 40–70 år kan ha stor betydelse för bedömningar i frågor som rör den svenska utrikes-, försvars- och säkerhetspolitiken. I den militära säkerhetstjänsten måste Försvarmakten t.ex. kunna behandla uppgifter om en anställd som genomgått registerkontroll under hela den tid personen är anställd inom myndigheten, vilket innebär att myndigheten måste kunna spara uppgifterna i minst 40 år.

Som exempel på det behov som finns inom Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten att bevara uppgifter kan först nämnas den behandling som sker i Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK). I rutinerna Person och Handling finns biografiska underrättelser för försvarsunderrättelseverksamhet och säkerhetstjänst. Här finns uppgifter om t.ex. politiska och militära befattningshavare. Det är inte rimligt att enligt strikta tidsgränser gallra uppgifter om t.ex. en statschef eller parlamentariker i en annan stat. Uppgifter om en sådan företrädares verksamhet är ofta nödvändiga att ha tillgång till under lång tid, kanske under personens hela livstid, och kan också vara av värde bl.a. vid en tillbakablickande studie av utvecklingen i en viss stat. Det är vidare omöjligt att i förväg veta vilka uppgifter som kan vara viktiga för verksamheten i framtiden. Motsvarande behov av att bevara uppgifter föreligger naturligtvis även i Försvarets radioanstalts försvarsunderrättelseverksamhet, som även den innefattar biografisk underrättelseverksamhet. Hos Försvarets radioanstalt kan sådana personuppgifter förekomma i samtliga databaser.

I rutinen RK (registerkontroll) antecknas när en person har genomgått en registerkontroll enligt säkerhetsskyddslagen (1996:627). Beträffande personer som är placerade i säkerhetsklass 3 eller i de fall kontroll av personen genomförts med stöd av 14 § säkerhetsskyddslagen (terrorism) kan det dröja mer än 20 år innan en omkontroll sker, om personen i fråga innehar en befattning i samma säkerhetsklass. Det är härvid nödvändigt att

Försvarsmakten kan bevara uppgifter om den kontrollerade i minst 30 år.

Enligt 16 § i den nu gällande förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt skall personuppgifter gallras senast tio år efter den senast införda uppgiften om den registrerade, om det inte finns särskilda skäl. Inom säkerhetsunderrättelsetjänsten finns emellertid ofta behov av att följa upp personer under mycket längre tid än tio år och det är tveksamt om särskilda skäl kan anses föreligga för sådan behandling i alla de fall som erfordras. Det kan t.ex. finnas behov av att återigen följa upp en person som tidigare varit verksam i Sverige och som återkommer hit efter en längre tids bortovaro än tio år. När det gäller personal som tillhör Försvarsmakten förekommer det att personer följs under hela anställningstiden vid myndigheten. Den militära personalen tillbringar ofta hela sin yrkesverksamma tid vid myndigheten, vilken kan uppgå till 40 år. Med hänsyn härtill bör eventuell gallringstid för sådana uppgifter inte understiga 50 år.

I Försvarsmaktens informationsdatabas behandlas bl.a. uppgifter från Faktiva och från Janes information group (se avsnitt 5.3.1), vilka inhämtas genom prenumeration. När det gäller uppgifter från Faktiva behövs inga särskilda gallringstider, eftersom dessa uppgifter rensas automatiskt efter 90 dagar. I fråga om prenumerationerna på Janes och vissa nyhetsbrev skulle det vara olämpligt att ange en gallringstid. Janes tillhandahålls genom CD-skivor och uppdateras via Internet. Dessa prenumerationer är öppna för vem som helst inom organisationen och motsvaras närmast av böcker i ett bibliotek. Sådan information omfattas av 2 kap. 11 § tredje punkten tryckfrihetsförordningen, den s.k. biblioteksregeln, och utgör därmed inte allmän handling hos myndigheten. Enligt nämnda bestämmelse 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. Skyldighet att gallra kan således bara komma i fråga när det gäller allmänna handlingar, inte avseende information i bibliotek. Sådan information skall emellertid, i den mån den utgör personuppgifter, enligt huvudregeln i personuppgiftslagen rensas (förstöras) när den inte längre behövs för de ändamål för vilka den registrerats.

Gallring sker i första hand för att värna skyddet av den personliga integriteten. 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. Andra metoder med samma ändamål är t.ex. sekretessbestämmelser. Som vi tidigare framhållit gäller i den militära underrättelse- och säkerhetstjänsten och i Försvarets radioanstalts underrättelseverksamhet en mycket omfattande sekretess samt även i övrigt hårda säkerhetskrav för behandlade uppgifter. Dessa förhållanden gagnar skyddet för den personliga integriteten och talar också 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. Som exempel kan nämnas den för ett tag sedan högaktuella frågan om ersättning till tvångssteriliserade. Ett stort antal personer har efter många år nu fått upprättelse för tidigare allvarliga integritetskränkningar, just på grund av att de känsliga uppgifterna inte har förstörts, utan i stället bevarats och därigenom kunnat utgöra underlag för att rekonstruera historiska händelseförlopp.

Vidare bör offentlighetsprincipen och den minskade möjligheten till insyn i myndigheternas verksamhet för bl.a. forskning framhållas som skäl mot omfattande gallring i allmänhet inte minst i den militära underrättelse- och säkerhetstjänsten och i Försvarets radioanstalts underrättelseverksamhet.

Vid en samlad bedömning har vi mot denna bakgrund stannat för att inte föreslå några särskilda gallringsbestämmelser för de aktuella verksamheterna. Detta innebär att bestämmelserna i arkivlagen och personuppgiftslagen blir avgörande för frågan om bevarande och gallring i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet, oavsett om personuppgifterna behandlas i en databas eller inte. I praktiken innebär detta att allmänna handlingar som huvudregel skall bevaras och att de får gallras endast om Riksarkivet har tillåtit det. För andra uppgifter, dvs. sådana uppgifter som inte utgör eller ingår i allmänna handlingar, gäller i stället att de skall rensas (förstöras) när de inte längre behövs för de ursprungliga ändamålen med registreringen.

9.2 Utlämnande av uppgifter

9.2.1 Sekretess och utlämnande av uppgifter till utländsk myndighet eller internationell organisation

Vårt förslag: 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 lämnande uppgifter inte är till skada för svenska intressen.

För uppgifter som behandlas i Försvarsmaktens underrättelse- och säkerhetstjänst och i Försvarets radioanstalts underrättelseverksamhet gäller sekretess av olika skäl och av olika grad. Enligt 2 kap. 1 § sekretesslagen gäller sekretess för uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Enligt 2 § samma kapitel gäller sekretess för uppgift som angår verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

I 5 § förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt finns en bestämmelse som anger under vilka omständigheter uppgifter skall kunna lämnas ut trots att sekretess gäller för uppgifterna. Bestämmelsen har sekretessbrytande karaktär och reglerar inte på vilket sätt uppgifterna får lämnas ut, dvs. om det får ske genom utlämnande på papper eller i elektronisk form. Något konstitutionellt hinder mot att regeringen genom en förordning medger att annars sekretessbelagda uppgifter lämnas ut myndigheter emellan föreligger inte. Regeringen kan dock inte genom föreskrifter i en förordning sätta åt sidan bestämmelser i en lag som exklusivt reglerar uppgiftsutbytet mellan myndigheter (jfr. Regner m.fl., Sekretesslagen En kommentar, Suppl. 8, s. 14:9.).

För att främja internationellt samarbete inom underrättelse- och säkerhetstjänsten anser vi att en bestämmelse motsvarande 5 § i

förordningen om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt bör återfinnas i de av oss föreslagna förordningarna om behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten respektive i Försvarets radioanstalts underrättelseverksamhet (jfr. 3 § i förordningarna).

Formuleringen att utlämnandet skall tjäna den svenska statsledningen och det svenska totalförsvaret är hämtad från förarbetena till lagen om försvarsunderrättelseverksamhet där syftet med försvarsunderrättelseverksamhetens utlandssamarbete slås fast (prop. 1999/2000:25 s. 11). Även om våra författningsområden är begränsat till automatiserad behandling av personuppgifter och uppgifter i strukturerade manuella register, så är de sekretessbrytande bestämmelserna i princip tillämpliga även om uppgifterna skulle lämnas ut på papper utan att ingå i ett strukturerat manuellt register. Bestämmelsen reglerar således inte formen för utlämnandet.

9.2.2 Utlämnande av uppgifter på medium för automatiserad behandling

Vårt förslag: Utlämnande av uppgifter på medium för automatiserad behandling i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarmaktens underrättelseverksamhet skall inte regleras särskilt.

Uppgifter kan lämnas ut från den militära underrättelse- och säkerhetstjänsten eller Försvarets radioanstalt på flera olika sätt. Utlämnande av uppgifter kan ske på traditionellt sätt i muntlig eller skriftlig form. Utlämnande kan också ske i elektronisk form på medium för automatiserad behandling, t.ex. genom användning av e-post, genom utlämnande på diskett eller cd-rom, eller genom direktåtkomst. Av dessa olika varianter är direktåtkomsten den mest känsliga och den behandlas därför särskilt i avsnitt 8.3.6.

Att ett utlämnande sker på *medium för automatiserad behandling* innebär att informationen lämnas ut i elektronisk form på ett sådant sätt att mottagaren kan bearbeta informationen.

En av de viktigare bestämmelserna i dataskyddsdirektivet och personuppgiftslagen är att uppgifter skall samlas in för särskilda,

uttryckliga och berättigade ändamål. Senare behandling får inte ske på ett sätt som är oförenligt med de ändamålen. Bestämmelsen innebär att en uppgift som har samlats in för ett visst ändamål inte får lämnas ut, om utlämnandet är oförenligt med det ursprungligen angivna ändamålet. Även om dataskyddsdirektivet inte är tillämpligt på de aktuella verksamheterna hos Försvarmakten och Försvarets radioanstalt gäller personuppgiftslagens bestämmelser i denna del för de båda myndigheterna. Detta innebär att allt utlämnande av personuppgifter måste stå i överensstämmelse med – eller i vart fall inte vara oförenligt med – de olika ändamål som gäller för behandling av personuppgifterna. Dock gäller att uppgifter oavsett ändamålen får lämnas ut med stöd av offentlighetsprincipen. Varken dataskyddsdirektivet eller personuppgiftslagen innehåller emellertid några uttryckliga bestämmelser som reglerar om eller under vilka förutsättningar uppgifter som omfattas av lagens tillämpningsområde får lämnas ut automatiserat. I det avseendet görs med andra ord ingen åtskillnad mellan elektroniskt och manuellt utlämnande.

I 7 kap. 16 § sekretesslagen (1980:100) anges att sekretess gäller för uppgifter om det kan antas att ett utlämnande skulle medföra att uppgifterna behandlas i strid med personuppgiftslagen. Med behandling av personuppgifter avses enligt personuppgiftslagen emellertid varje åtgärd som vidtas med uppgiften. Det saknar därför även ur sekretesslagens synvinkel direkt betydelse om utlämnandet av en uppgift görs automatiserat eller manuellt på papper, eftersom utlämnandet under alla förhållanden omfattas av 7 kap. 16 § om uppgiften efter utlämnandet kan komma att behandlas automatiserat eller i manuella register i strid mot personuppgiftslagens bestämmelser. Bestämmelsen i sekretesslagen ses för närvarande över av Utredningen om översyn av personuppgiftslagen (dir. 2002:31).

När det gäller den militära underrättelse- och säkerhetstjänsten samt Försvarets radioanstalt torde utlämnande förekomma till annan svensk myndighet och till annan stat eller internationell organisation inom ramen för det internationella underrättelse- och säkerhetssamarbetet.

För myndigheter finns ofta särskilda registerförfattningar som reglerar vilka personuppgiftssamlingar som får föras av myndigheten och på vilket sätt personuppgifter får behandlas. I de författningarna regleras även ändamålen med behandlingen. Vi bedömer därför att riskerna är små för att en myndighet som får personuppgifter i elektronisk form eller på annat sätt från

Försvarsmakten eller Försvarets radioanstalt, skall behandla uppgifterna på ett otillåtet sätt. Samtidigt är det klart att det innebär stora effektivitetsvinster för myndigheter att hämta in uppgifter som skall behandlas automatiserat genom automatiserade förfaranden, t.ex. på diskett eller via telenätet.

Inom ramen för myndigheternas internationella samarbete ställs med hänsyn till verksamheternas art mycket höga säkerhetskrav för att utlämnande skall få ske. Kan dessa säkerhetskrav inte efterlevas sker inte utlämnande på medium för automatiserad behandling, utan i stället t.ex. i pappersform. Huruvida ett utlämnande på medium för automatiserad behandling skall få ske får i detta sammanhang helt avgöras mot bakgrund av försvars- och säkerhetspolitiska ställningstaganden. Utländska mottagare är till skillnad från svenska myndigheter nämligen inte bundna av personuppgiftslagen och 7 kap. 16 § sekretesslagen är därmed inte tillämplig.

En utgångspunkt för vårt arbete har varit att Försvarsmakten och Försvarets radioanstalt skall kunna utnyttja automatiserade förfaranden och i övrigt bedriva de aktuella verksamheterna med ett rationellt datorstöd, naturligtvis under förutsättning att det inte medför risk för otillbörliga intrång i enskildas personliga integritet. Den slutsats som kan dras av det ovan anförda är att det inte finns något rättsligt krav på att författningsreglera utlämnande som sker på medium för automatiserad behandling. Inte heller verksamheten som sådan ger enligt vår uppfattning anledning att särskilt reglera utlämnande enbart på den grunden att utlämnandet sker på medium för automatiserad behandling. De säkerhetskrav som betingas av ändamålet med verksamheten medför att det inte föreligger någon större risk för att uppgifter lämnas ut på medium för automatiserad behandling till andra myndigheter eller inom det internationella samarbetet på ett otillbörligt sätt. I föregående avsnitt lämnar vi förslag på en sekretessbrytande bestämmelse som skall möjliggöra utlämnande till utländska myndigheter och internationella organisationer. Är det med hänsyn till dessa bestämmelser tillåtet att lämna ut uppgifterna bör myndigheten på egen hand få avgöra formerna för ett sådant utlämnande. En förutsättning är emellertid att den utlämnande myndigheten har möjlighet att i varje enskilt fall avgöra vilka uppgifter som skall lämnas ut, vilket inte är fallet när uppgifter lämnas ut genom direktåtkomst (se avsnitt 8.3.6).

10 Sekretessfrågor

10.1 Sekretess till skydd för enskilds personliga eller ekonomiska förhållanden

Vårt förslag: I sekretesslagen (1980:100) skall införas en bestämmelse om sekretess hos Försvarmakten i den militära underrättelse- och säkerhetstjänsten till skydd för uppgift om enskilds personliga eller ekonomiska förhållanden.

Sekretess för sådan uppgift skall gälla om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men.

Sekretess skall gälla i högst 70 år.

Försvarmakten behandlar i åtskilliga fall uppgifter som är mycket känsliga med hänsyn till enskildas personliga förhållanden. Detta kommer naturligtvis att ske automatiserat med stöd av den lag om behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten som vi nu föreslår, men det kan förekomma även i andra sammanhang inom den militära underrättelse- och säkerhetstjänsten t.ex. i manuella register eller vanliga pappersdokument.

Exempel på sådana uppgifter kan vara politiska åsikter, etniskt ursprung, sexuell läggning m.m. Vidare kan det tänkas förekomma uppgifter om enskilds fysiska eller psykiska hälsa liksom om enskilds familjeförhållanden. Säkerligen kan också uppgifter om enskildas ekonomiska förhållanden komma att behandlas. Det kan även komma ifråga att behandla uppgifter om lagöverträdelse, och i den militära säkerhetstjänsten kan det finnas behov av att behandla uppgifter om att en person misstänks för brott. Ett utlämnande av sådana uppgifter skulle kunna vara till skada eller

men för såväl den enskilde själv som för närstående till den som uppgifterna rör.

De personer om vilka det förekommer uppgifter i den militära underrättelse- och säkerhetstjänsten är ofta politiska beslutsfattare eller militära befattningshavare i en annan stat. Även uppgifter om andra enskilda privatpersoner kan dock förekomma, t.ex. efter att de uppträtt som uppgiftslämnare eller på annat sätt har haft anknytning till den aktuella verksamheten.

Vi har uppmärksammat det faktum att det i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten finns uppgifter som kan vara mycket integritetskänsliga och som inte skyddas av gällande sekretessregler. Vi har mot bakgrund härav funnit anledning att se över de sekretessregler som nu gäller för att undersöka om det finns skäl att förstärka sekretesskyddet för uppgifter hos den militära underrättelse- och säkerhetstjänsten om enskilds personliga eller ekonomiska förhållanden.

Sekretess i den militära underrättelse- och säkerhetstjänsten

I de flesta fall föreligger sekretess för uppgifterna hos den militära underrättelse- och säkerhetstjänsten enligt reglerna om utrikes- och/eller försvarssekretess i 2 kap. 1 och 2 §§ sekretesslagen (1980:100). Enligt 2 kap. 1 § sekretesslagen gäller sekretess för uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Utrikessekretessen har givetvis sin största betydelse för regeringen, Regeringskansliet och utrikesrepresentationen men den gäller för samtliga statliga myndigheter.

Enligt 2 § samma kapitel gäller sekretess för uppgift som angår verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Det sekretessbelagda området omfattar inte bara rent militära företeelser utan också åtgärder med avseende på totalförsvaret i övrigt. Försvarssekretess gäller vid antagna skador inte endast mot landets försvar i vedertagen mening utan också mot rikets säkerhet på annat sätt. I fråga om uppgift i allmän handling gäller såväl utrikes- som

försvarssekretessen i högst 40 år. Om särskilda skäl föranleder det får dock regeringen, när det gäller försvarssekretess, föreskriva att sekretessen skall gälla under längre tid. Även försvarssekretessen gäller inom hela det allmännas verksamhet, men har naturligtvis störst betydelse hos Försvarsmakten och andra myndigheter med anknytning till försvaret, t.ex. Försvarets radioanstalt.

Den utrikes- och försvarssekretess som gäller i den militära underrättelse- och säkerhetstjänsten syftar endast till att skydda själva verksamheten hos myndigheten och utgör härmed inget skydd för enskilda individer och deras personliga eller ekonomiska intressen. Sekretessen enligt 2 kap. 1–2 §§ sekretesslagen gäller vanligtvis i högst 40 år. Detta innebär att uppgifter som kommit Försvarsmakten tillhanda t.ex. under andra världskriget, och även ett antal år därefter, inte längre omfattas av sekretess, såvida regeringen inte fattat särskilt beslut härom. När det gäller skyddet av enskildas personliga förhållanden kan det finnas anledning att sekretessen gäller även efter det att sekretess till skydd för det allmänna har upphört. Regeringens möjlighet att föreskriva om sekretess utöver 40 år tar emellertid även den endast sikte på sekretess till skydd för verksamheten.

Såväl i försvarsunderrättelseverksamhet som i den militära säkerhetstjänsten kan förekomma att en rapportör lämnar förtrolig information till Försvarsmakten om personer denne känner väl. Det kan röra sig om uppgifter som t.ex. avslöjar personens hälsotillstånd eller familjeförhållanden, och som skulle medföra skada eller men för den enskilde om uppgifterna lämnas ut. I något fall har t.ex. en hel sjukjournal lämnats in. Någon bestämmelse om sekretess som tar sikte på skyddet för den personliga integriteten i detta sammanhang finns inte. I det fall sekretess inte kan göras gällande till skydd för det allmänna finns det ingen regel om sekretess som direkt omfattar dessa uppgifter.

I den militära säkerhetstjänstens verksamhet kan det förekomma uppgifter om en anställds missbruksproblem eller andra personliga förhållanden som gör att den anställda kan anses vara mindre lämpad att betros med hemliga uppgifter. Dessa personuppgifter kan t.ex. komma från den anställda själv eller från den personaladministrativa verksamheten vid det förband där vederbörande är placerad. Nämnade uppgifter skulle eventuellt kunna vara skyddade enligt bestämmelsen i 7 kap. 11 § sekretesslagen (1980:100) om sekretess i myndighetens personaladministrativa verksamhet. Den militära säkerhetstjänstens verksamhet kan emellertid inte alltid hänföras till personaladministrativ verksamhet, även om det gäller

personal i Försvarsmakten. Bestämmelsen ger därför inte ett tillräckligt skydd för uppgifter om enskilda personliga förhållanden.

Mot bakgrund härav finns det enligt vår uppfattning anledning att säkerställa att uppgifter om enskilda personliga förhållanden får ett fullgott sekretessskydd hos den militära underrättelse- och säkerhetstjänsten. Även uppgifter om juridiska personer kan behandlas i stor omfattning inom den militära underrättelse- och säkerhetstjänsten. Det finns därför skäl att anta att ett offentliggörande av vissa uppgifter kan komma att skada t.ex. ett företag eller annan organisation. Vi anser därför att en bestämmelse bör utformas så att den möjliggör sekretess även för uppgift om enskilda ekonomiska förhållanden. Detta ligger också i linje med vårt förslag att lagen om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och i den militära säkerhetstjänsten skall omfatta även juridiska personer. Annat har inte framkommit än att den sekretess som gäller till skydd för det allmännas intresse är tillräcklig. Någon ytterligare bestämmelse till skydd för detta intresse föreslås därför inte.

Sekretess i liknande verksamheter

När det gäller behovet av skydd för uppgifter om enskildas personliga eller ekonomiska förhållanden är det enligt vår mening av intresse från jämförelsesynpunkt att se vad som gäller hos bl.a. polisen i detta hänseende. Enligt 5 kap. 1 § gäller sekretess för uppgift som hänför sig till sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terrorism. Sekretess gäller om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Enligt 7 kap. 17 § sekretesslagen gäller sekretess för uppgift i register som förs med stöd av lagen (1998:620) om belastningsregister. Uppgift i ett register som förs enligt lagen om belastningsregister kan endast lämnas ut om det är särskilt föreskrivet i den lagen, säkerhetsskyddslagen eller i förordningar som har stöd i dessa lagar. För uppgift som finns i allmän handling gäller sekretessen i högst 70 år.

I 9 kap. 17 § sekretesslagen finns en korresponderande sekretessregel till 5 kap. 1 § till skydd för enskildas personliga eller ekonomiska förhållanden. I bestämmelsen föreskrivs att sekretess

gäller i ett antal myndigheters brottsförebyggande och brottsbeivrande verksamhet. I bestämmelsen finns bl.a. regler om sekretess för uppgifter i register som förs av Rikspolisstyrelsen enligt polisdatalagen (1998:622) och lagen (1998:621) om miss-tankeregister. Några av bestämmelserna i paragrafen är så utformade att de i undantagsfall även kan komma ifråga för Försvarsmakten att tillämpa. De kan dock inte sägas ge ett godtagbart skydd för uppgifter om enskilda i den militära underrättelse- och säkerhetstjänsten och tar heller inte sikte på sådan verksamhet. Sekretess gäller 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 70 år.

I 9 kap. 26 § sekretesslagen finns sedan den 1 januari 2000 en bestämmelse om sekretess hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet. Bestämmelser om kommissionen och dess verksamhet finns i lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet. Kommissionen har i december 2002 slutfört sitt uppdrag (SOU 2002:87–95). Föremålet för sekretess är enligt nyss nämnda bestämmelse i sekretesslagen uppgift om enskildas personliga eller ekonomiska förhållanden. Det kan utöver uppgifter om ekonomi och hälsa röra sig om t.ex. uppgifter om politisk hemvist eller samreöre med vissa politiska grupper. Sekretess gäller med ett omvänt skaderekvisit, dvs. det är presumtion för sekretess och uppgifter får röjas endast om det står klart att så kan ske utan att en enskild eller någon honom närstående lider skada eller men. Sekretesstiden för uppgifter i allmänna handlingar är högst 70 år. Sekretessen avser uppgifter som kommissionen inhämtat vid sin granskning av bl.a. den militära underrättelse- och säkerhetstjänsten.

Som vi pekat på finns inte någon motsvarande bestämmelse för den militära underrättelse- och säkerhetstjänsten. Detta kan innebära att en uppgift som inte omfattades av sekretess när den fanns hos den militära underrättelse- och säkerhetstjänsten blivit belagd med sekretess efter det att den överlämnats till kommissionen. Det framstår med hänsyn härtill närmast som ett förbiseende att det inte redan finns en bestämmelse om sekretess för den militära underrättelse- och säkerhetstjänsten. Enligt vår uppfattning föreligger det minst lika goda skäl för sekretess till skydd för enskildas personliga eller ekonomiska förhållanden i själva verksamheten som hos granskningsorganet.

Skaderekvisit

Fråga är om vilken typ av skaderekvisit som bör gälla enligt den bestämmelse vi föreslår. En sekretessbestämmelse kan gälla utan skaderekvisit, eller med ett omvänt eller rakt skaderekvisit. När skaderekvisit saknas sägs vanligen att absolut sekretess råder. Sekretessen är emellertid inte absolut, eftersom den viker om uppgiftsskyldighet följer av lag eller förordning (se 14 kap. 1 § sekretesslagen). Rakt skaderekvisit innebär att offentlighet är huvudregel och att sekretess gäller endast om det kan antas att ett röjande medför skada eller men. Med ett omvänt skaderekvisit råder presumtion för sekretess och uppgiften får röjas endast om det står klart att så kan ske utan att en enskild eller någon honom närstående lider skada eller men.

Bestämmelser om "absolut" sekretess är ovanliga. När det gäller kriminalunderrättelseregister och Säkerhetspolisens register har regeringen ansett att absolut sekretess inte är motiverad, eftersom det finns utomstående som har ett berättigat intresse till insyn i registren. För att allmänheten skall ha förtroende för den underrättelseverksamhet som bedrivs av såväl den öppna polisen som Säkerhetspolisen är det viktigt att det dessutom finns tillräckliga möjligheter till insyn i och kontroll av de register som förs. Med hänsyn till att uppgifter i de register som nu nämnts är mycket känsliga från integritetssynpunkt har regeringen dock ansett det självklart att uppgifterna bör omgärdas av ett starkt sekretesskydd. Bestämmelserna i 9 kap. 17 § sekretesslagen har därför försetts med ett omvänt skaderekvisit, vilket innebär att uppgifter får lämnas ut endast om det står klart att det inte medför någon skada för den enskilde eller någon honom närstående (prop. 1997/98:97 s. 67).

Enligt 9 kap. 26 § sekretesslagen, som avser sekretess hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet, och i vilken paragraf föremålet för sekretessen är uppgifter om enskildas personliga eller ekonomiska förhållanden gäller ett omvänt skaderekvisit.

Den allmänna försvarssekretessen är utformad med ett rakt skaderekvisit. Skälet härtill är att man velat undvika ett onödigt hemlighållande av uppgifter inom de många olika verksamhetsområden och företeelser som försvarssekretessen omfattar. Vårt förslag omfattar endast sådana uppgifter inom Försvarsmakten som förekommer i den militära underrättelse- och säkerhetstjänsten och som därmed kan antas vara av särskilt känslig natur för enskilda

och deras närstående. Enligt vår uppfattning bör därför sekretess vara huvudregel i enlighet med vad som gäller hos polisen och säkerhetstjänstkommissionen och en bestämmelse bör således vara förenad med ett omvänt skaderekvisit.

Vi är medvetna om att det i olika sammanhang har riktats kritik mot sekretess som är förenad med ett omvänt skaderekvisit, bl.a. när det gäller 9 kap. 17 § sekretesslagen där rekvisitet har medfört vissa olägenheter främst för domstolarna (jfr. Ds 2002:29 s. 24). Liknande olägenheter gör sig emellertid inte gällande i förevarande sammanhang. Det kan vidare anföras att det är viktigt att uppgifter inte undanhålls allmänhetens insyn mer än vad som är nödvändigt, t.ex. med hänsyn till rikets säkerhet, brottsförebyggande och brottsbeivrande verksamhet samt enskildas personliga förhållanden, och att ett omvänt skaderekvisit kan medföra en onödigt stark sekretess. Vad vi föreslår är emellertid inte någon generell inskränkning i offentligheten. Uppgifter hos Försvarsmakten skyddas i första hand av utrikes- och försvarssekretessen. Som framgått behövs det dock i vissa fall regler om sekretess till skydd för enskildas personliga eller ekonomiska förhållanden. Det finns ingen möjlighet att göra gällande försvarssekretess för uppgifter som inkommit till Försvarsmakten enbart av den anledningen att uppgifterna är mycket känsliga för enskilda individer.

Vi har övervägt att förena en sekretessbestämmelse med ett rakt skaderekvisit. Enligt vår uppfattning talar emellertid övervägande skäl för att den bestämmelse vi föreslår skall utformas med samma skaderekvisit som gäller i jämförbara verksamheter, som t.ex. polisens verksamhet. Således bör en bestämmelse om sekretess till skydd för enskilds personliga och ekonomiska förhållanden i den militära underrättelse- och säkerhetstjänsten vara förenad med ett omvänt skaderekvisit, vilket innebär att sekretess är huvudregel och att uppgifter får röjas endast om det står klart att så kan ske utan att den enskilde eller någon honom närstående lider skada eller men.

Sekretessens omfattning

Vi har diskuterat om bestämmelsen om sekretess endast skall omfatta de uppgifter som behandlas automatiserat i den aktuella verksamheten. Enligt vår uppfattning bör emellertid inte någon sådan uppdelning göras eftersom den militära underrättelse- och säkerhetstjänstens behandling av uppgifter inte uteslutande är

koncentrerad till automatiserade uppgiftssamlingar utan känsliga uppgifter kan förekomma i manuella register och i vanliga pappersdokument. En fördel med att inte ha en sådan uppdelning blir också att samma sekretesskydd kommer att gälla för uppgiften oavsett om den förekommer i ett automatiserat register eller figurerar på annat sätt. På så sätt uppkommer inga gränsdragningsproblem i sekreteshänseende.

Sekretesstidens längd

I fråga om sekretess till skydd för det allmännas verksamhet varierar sekretesstiderna. För uppgift i allmän handling som hänför sig till sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som annars hänför sig till Säkerhetspolisens verksamhet för att förebygga brott mot rikets säkerhet eller förebygga terrorism gäller enligt 5 kap. 1 § sekretesslagen sekretessen i högst 70 år. Sekretesstiden för uppgifter om enskilda personliga och ekonomiska förhållanden är i dessa fall också 70 år (9 kap. 17 § sekretesslagen).

Hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet är enligt 9 kap. 26 § sekretesslagen sekretesstiden för uppgifter i allmänna handlingar högst 70 år.

För uppgifter för vilka utrikes- och försvarssekretess gäller kan sekretess föreligga i högst 40 år (2 kap. 1 och 2 §§ sekretesslagen). När det gäller uppgifter som omfattas av försvarssekretess har emellertid regeringen bemyndigats att föreskriva att sekretessen skall gälla under längre tid. Detta bemyndigande har regeringen utnyttjat och i 1 § sekretessförordningen (1980:657) föreskrivit att sekretessen gäller i högst 70 år om uppgifterna i en allmän handling angår bl.a. underrättelseverksamheten inom underrättelse- och säkerhetstjänsten.

I propositionen om ny sekretesslag föreslog regeringen att en sekretesstid om 70 år skulle gälla för de viktigaste bestämmelserna om skydd för enskilda personliga förhållanden (prop. 1979/80:2 del A s. 493f.). Genom den ändring som gjordes i sekretesslagen i samband med polisdatalagens införande tidsbegränsades sekretessen i polisregister till skydd för polisens verksamhet till 70 år. I förarbetena anförde regeringen att sekretesstidens längd borde motsvara den som normalt gäller till skydd för enskilda personliga förhållanden (prop. 1997/98:97 s. 69).

I samband med frågan om gallring i 9 kap. framför vi att det är av stor betydelse för den militära underrättelse- och säkerhetstjänsten att kunna spara uppgifter och handlingar under en så lång tid som upp till 70 år. Med hänsyn härtill och mot bakgrund av att denna tid är vad som normalt gäller vid sekretess till skydd för enskilda personliga förhållanden bör sekretess hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten till skydd för uppgift om enskilda personliga eller ekonomiska förhållanden gälla i högst 70 år.

Sedan den 1 mars 2003 gäller att sekretess till skydd för enskildas personliga eller ekonomiska förhållanden enligt 9 kap. 17 § första stycket 1–4 och 6 sekretesslagen inte längre skall gälla avseende uppgifter hos Säkerhetspolisen från tiden före 1949 (prop. 2001/02:191). Det kan därför ifrågasättas om man för uppgifter hos den militära underrättelse- och säkerhetstjänsten nu skall införa en sekretesstid om 70 år. I nämnda proposition framhålls att regeringen avser att tillsätta en utredning med uppgift att se över vad som krävs för att möjliggöra en ökad offentlighet för sådana uppgifter hos Försvarsmakten som angår underrättelseverksamheten inom underrättelse- och säkerhetstjänsten och som hänför sig till tiden för andra världskriget (a.a. s. 87). Vi finner därför inte skäl att nu föreslå annat än att sekretess till skydd för enskilda personliga eller ekonomiska förhållanden för uppgift i den militära underrättelse- och säkerhetstjänsten bör gälla i högst 70 år. Den förutskickade utredningen har möjlighet att närmare överväga om sekretesstiden skall begränsas.

Sammanfattning

Mot bakgrund av vad som anförts ovan föreslår vi att det i sekretesslagen bör införas en ny bestämmelse om sekretess hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten till skydd för uppgift om enskilda personliga eller ekonomiska förhållanden. Sekretess för sådan uppgift bör 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.

11 Ikraftträdande- och övergångsbestämmelser

Vårt förslag: Lagen om behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten och lagen om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet samt de kompletterande förordningarna och de ändringar vi föreslår i andra författningar, skall träda i kraft den 1 juli 2004.

Samtidigt med att de nya lagarna och förordningarna träder i kraft skall den förordning som i dag reglerar behandlingen av personuppgifter inom Försvarmakten och Försvarets radioanstalt upphöra att gälla.

Bestämmelser i de nya lagarna 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 av personuppgifter, som utförs för ett visst bestämt ändamål, om manuell behandling för ändamålet påbörjats före den 24 oktober 1998.

Den nya lagstiftning vi föreslår för behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet bör kunna träda i kraft den 1 juli 2004. Detsamma gäller de kompletterande förordningarna samt de ändringar vi föreslår i sekretesslagen (1980:100) och förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd. Samtidigt bör förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt upphöra att gälla.

För manuell behandling skall personuppgiftslagen (1998:204) inte börja tillämpas fullt ut förrän den 1 oktober 2007. Våra författningsförslag omfattar sådan manuell behandling som i avsaknad av särskild lagstiftning skulle omfattas av personuppgiftslagens bestämmelser. Det saknas enligt vår uppfattning anledning att låta manuell behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet omfattas av lagstiftningen i annan utsträckning än vad som skulle ha varit fallet om endast personuppgiftslagens bestämmelser hade varit tillämpliga. De undantag från tillämpning fram till den 1 oktober 2007 som föreskrivs i personuppgiftslagen avseende manuella register, som påbörjats redan före den lagens ikraftträdande, bör därför gälla även för behandling enligt den av oss nu föreslagna lagstiftningen. I praktiken torde dock övergångsbestämmelsen sakna eller ha mycket begränsad betydelse.

I övrigt gör vi den bedömningen att behandling av personuppgifter och andra uppgifter som i dag utförs i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet utan ytterligare övergångsbestämmelser direkt kan omfattas av bestämmelserna i den nya lagstiftningen när den träder i kraft.

12 Konsekvenser av våra förslag

Vår bedömning: Våra förslag kommer att ge förutsättningar för myndigheterna att bedriva sin verksamhet effektivt och med ett rationellt datorstöd. Förslagen innebär en flexibel reglering som ger myndigheterna möjlighet att fortlöpande utveckla och anpassa sina system för automatiserad behandling av personuppgifter utan att det fordrar ändringar i regelverket. Förslagen i sig medför inte några kostnadsökningar.

Kommittéer som tillkallats på grund av ett regeringsbeslut och som har ett utredningsuppdrag skall enligt kommittéförordningen (1998:1474) genomföra konsekvensanalyser i skilda hänseenden beträffande de förslag som framställts. Vad som sägs i förordningen om kommittéer gäller också särskilda utredare. Om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, skall en beräkning av dessa konsekvenser redovisas i betänkandet.

Om förslagen innebär samhällsekonomiska konsekvenser i övrigt skall dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller landsting, skall kommittén eller utredaren föreslå en finansiering. Om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, skall konsekvenserna också i det avseendet anges i betänkandet. Detsamma gäller när ett förslag har betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

En grundläggande utgångspunkt för vårt arbete har varit att föreslå moderna, teknikneutrala och allmänt ändamålsenliga bestämmelser. Särskild hänsyn har tagits till de integritetsaspekter som följer av omfattande automatiserade uppgiftssamlingar i myndighetsverksamhet. En annan viktig utgångspunkt för vårt arbete har varit att våra förslag i möjligaste mån skall underlätta samverkan mellan de svenska myndigheter som bedriver försvarsunderrättelseverksamhet och/eller säkerhetstjänst. Förslagen är vidare ägnade att främja det internationella försvarsunderrättelse- och säkerhetssamarbetet mellan Försvarsmakten samt Försvarets radioanstalt och andra staters myndigheter eller internationella organisationer.

Våra författningsförslag kommer inte att innebära några kostnader för Försvarsmaktens eller Försvarets radioanstalts pågående verksamhet, eftersom de befintliga datorsystemen kan bibehållas. Förslagen innebär en lagstiftning som är teknikneutral. Våra förslag tillåter härigenom att nya datorsystem i framtiden kan tillskapas utan att det blir nödvändigt att ändra regelverket. Våra förslag innebär att Försvarsmakten och Försvarets radioanstalt ges frihet att välja i vilken omfattning myndigheterna vill inrätta ett eller flera nya register eller system inom ramen för de gemensamma databaserna.

Vid en jämförelse med vad som gäller i dag, innebär våra förslag också en större flexibilitet i fråga om möjligheterna till informationsutbyte mellan myndigheter. Vi föreslår t.ex. att Regeringskansliet, Försvarets materielverk, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Tullverket och Krisberedskapsmyndigheten i viss omfattning skall ges direktåtkomst till Försvarsmaktens databaser. På motsvarande sätt föreslår vi att Regeringskansliet och Försvarsmakten skall få ha viss direktåtkomst till Försvarets radioanstalts rapportdatabas. Förslagen om direktåtkomst kan förväntas medföra besparingar genom de effektivitetsvinster som direktåtkomsten åstadkommer. De myndigheter som bedriver försvarsunderrättelseverksamhet kan genom direktåtkomsten utföra sitt arbete på ett mer effektivt sätt.

Vissa utbildningsinsatser kan komma att krävas, men vi bedömer att dessa, jämfört med den fortlöpande vidareutbildningen av personalen inom Försvarsmakten och Försvarets radioanstalt, inte är mer omfattande än att de kan täckas av ordinarie utbildningsanslag.

Enligt våra förslag skall Försvarets underrättelsenämnd få i särskild uppgift att granska den behandling av uppgifter som sker

med stöd av de författningar vi föreslår. Enligt vår bedömning kan denna granskning genomföras i samband med den mycket närliggande kontroll som nämnden redan i dag har att utföra. Vårt förslag i denna del bör därför inte rimligen leda till några egentliga kostnadsökningar för staten.

13 Författningskommentarer

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

1 kap. Allmänna bestämmelser

1 §

Enligt *första stycket* skall lagen, liksom personuppgiftslagen, tillämpas på all behandling av personuppgifter som är helt eller delvis automatiserad samt viss strukturerad manuell behandling. Med personuppgifter avses detsamma som i personuppgiftslagen, nämligen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Begränsningen till försvarsunderrättelseverksamhet och militär säkerhetstjänst innebär en avgränsning mot Försvarmaktens övriga verksamheter. Vad som är försvarsunderrättelseverksamhet respektive militär säkerhetstjänst legaldefinieras inte, men ledning kan hämtas i 5–7 §§ om för vilka ändamål uppgifter får behandlas. Utanför lagens tillämpningsområde faller även behandling av personuppgifter i samband med de interna och administrativa åtgärder som kan förekomma i Försvarmaktens verksamhet. För behandling av uppgifter som rör sådana frågor, t.ex. i personal- och löneregister, gäller i stället personuppgiftslagen.

Enligt *andra stycket* skall bestämmelserna om personuppgiftsansvar, ändamål samt de bestämmelser som gäller myndighetens databaser i de aktuella verksamheterna, tillämpas också på juridiska personer.

Bestämmelserna i 1 kap. är generella och gäller, om inte annat sägs, för all behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten, oavsett om det gäller e-post, enskilda tjänstemäns promemorior

som upprättas i ordbehandlingsprogram, mindre register som används tillfälligt i underrättelseprojekt eller större register och datorsystem som används gemensamt i verksamheterna.

I *tredje stycket* upplyses om att det i 2 kap. finns särskilda bestämmelser för behandling av personuppgifter i den militära underrättelse- och säkerhetstjänstens databaser.

(*Se avsnitt 8.2.1*)

2 §

Lagen gäller i stället för personuppgiftslagen (1998:204). I de fall bestämmelser i personuppgiftslagen är tillämpliga även på behandling i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten anges det särskilt.

(*Se avsnitt 8.2.2*)

3 §

I paragrafen anges vilka bestämmelser i personuppgiftslagen som skall vara tillämpliga även vid behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten. De angivna bestämmelserna är alltså inte tillämpliga på behandling av uppgifter om juridiska personer.

(*Se avsnitt 8.2.2*)

4 §

Försvarmakten är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför. Personuppgiftsansvaret gäller även vid underlåtenhet att utföra en behandling som åligger Försvarmakten. Med personuppgiftsansvaret följer en rad skyldigheter. Den personuppgiftsansvarige skall bl.a. se till att behandlingen av uppgifter sker på ett korrekt och säkert sätt samt att information lämnas till den registrerade.

Försvarmakten har även ansvar för uppgifter om juridiska personer, dvs. sådant som inte utgör personuppgifter. Ansvaret innebär motsvarande skyldigheter som personuppgiftsansvaret i fråga om de krav som lagen ställer på behandling av uppgifter om juridiska personer, t.ex. att uppgifterna endast får behandlas för tillåtna ändamål. Även ansvaret för att de krav som ställs upp i lagens 2 kap. för behandling av uppgifter i myndighetens databaser uppfylls, gäller för uppgifter om juridiska personer. Däremot är bestämmelserna i 3 kap. om enskildas rättigheter inte tillämpliga, vilket t.ex. innebär att Försvarmaktens ansvar gentemot juridiska

personer inte omfattar skyldighet att lämna information eller rätta uppgifter enligt personuppgiftslagen.
(Se avsnitt 8.2.3)

5 §

Paragrafen anger de ändamål för vilka uppgifter får användas – dvs. samlas in, registreras, lämnas ut och i övrigt behandlas – i Försvarsmaktens försvarsunderrättelseverksamhet. Bestämmelsen tillämpas på uppgifter om såväl fysiska som juridiska personer.

Enligt lagen (2000:130) om försvarsunderrättelseverksamhet och den anslutande förordningen (2000:131) åligger det Försvarsmakten att bedriva försvarsunderrättelseverksamhet för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Försvarsunderrättelseverksamheten är ett led i Försvarsmaktens uppgifter att i fred, under beredskap och i krig ge underlag för Försvarsmaktens beredskap, operativa verksamhet och förbandsproduktion samt för krigsorganisationens utveckling och materiella förnyelse. Försvarsunderrättelseverksamhet består av inhämtning, bearbetning och analys samt delgivning av information. Härigenom utarbetas hotbildsanalyser och underrättelsebedömningar som delges Regeringskansliet och andra berörda myndigheter. Det är regeringen som bestämmer den närmare inriktningen av försvarsunderrättelseverksamheten.

Enligt *punkten 1* får uppgifter behandlas för säkerhetspolitiska och militärstrategiska bedömningar. Försvarsunderrättelseverksamheten skall identifiera och redovisa eller ge förvarning om sådana förändringar i omvärldsläget att detta kan ligga till grund för politiska beslut om totalförsvarets anpassning på kort eller lång sikt. Totalförsvaret är den verksamhet som behövs för att förbereda Sverige för krig och består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar), se 1 § lagen (1992:1403) om totalförsvaret och höjd beredskap.

Enligt *punkten 2* får uppgifter behandlas för den militära underrättelsetjänstens centrala uppgift att inom ramen för Försvarsmaktens grundberedskap upprätthålla försvar mot väpnat angrepp och för att hävda svensk territoriell integritet. Punkten 2 är också tillämplig vid behandling av uppgifter vid Sveriges deltagande vid internationella fredsbevarande och humanitära insatser, samt för att stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället. Det gäller att kunna förutse konflikter samt bearbeta inhämtat material och delge bedömningar om säkerhetspolitiska och militära förhållanden. Det

kan också röra sig om att medverka med information och analys i fråga om sådant som t.ex. internationell terrorism och gränsöverskridande miljöhot.

Med *punkten 3* avses personlig information om t.ex. militär personal, politiker eller andra viktiga befattningshavare. Sådana uppgifter är nödvändiga att behandla för att informationsunderlaget till stöd för svensk utrikes-, försvars- och säkerhetspolitik skall bli komplett.

(Se *avsnitt 2.4 och 8.2.4*)

6 §

Paragrafen anger de ändamål för vilka uppgifter får användas – dvs. samlas in registreras, lämnas ut och i övrigt behandlas – i den militära säkerhetstjänsten. Bestämmelsen tillämpas på uppgifter om såväl fysiska som juridiska personer.

Ändamålet med behandlingen av personuppgifter inom den militära säkerhetstjänsten är att Försvarsmakten skall kunna utföra de uppgifter som åligger myndigheten enligt säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633) och 4 § 2. förordningen (2000:555) med instruktion för Försvarsmakten. Uppgifter får behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen. Häri ingår bl.a. att biträda polisen i dess ansvar beträffande skyddet av rikets säkerhet. Den militära säkerhetstjänsten kan delas in i säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signal-skyddstjänst.

Enligt *punkten 1* får uppgifter behandlas för säkerhetsunderrättelsetjänst, som syftar till att klarlägga verksamhet som innefattar hot mot rikets säkerhet och personer med anknytning till sådan verksamhet. Denna verksamhet sker i stort under samma arbetsformer och med utnyttjande av samma typ av källor som används i försvarsunderrättelseverksamheten.

Inom säkerhetsskyddstjänsten, som nämns i *punkten 2*, vidtas olika åtgärder för att förhindra eller försvåra säkerhetshotande verksamhet. Härvid arbetar man med att förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Verksamheten syftar också till att skydda Försvarsmaktens personal, materiel och anläggningar.

Enligt *punkten 3* får uppgifter behandlas för ändamålet signal-skyddstjänst, som syftar till att minska verkan av signalspaning, falsk signalering och störsändning mot totalförsvarets telekommunikations- och informationssystem. Verksamheten skall förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikationer, samt användning av kryptografiska funktioner i informationssystemen. 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.
(Se *avsnitt 2.5 och 8.2.4*)

7 §

I paragrafen preciseras de ändamål för vilka personuppgifter får behandlas inom den militära säkerhetstjänsten med en särskild bestämmelse om vilka uppgiftskategorier som får behandlas i verksamheten. Uppgifter om en person får i huvudsak behandlas endast om personen misstänks för säkerhetshotande verksamhet eller har lämnat uppgift om sådan verksamhet samt om uppgifterna har framkommit genom att någon genomgått en registerkontroll enligt säkerhetsskyddslagen (1996:627).

Genom hänvisningen i första stycket till 6 § 1–2 undantas Försvarsmaktens signal-skyddstjänst från kraven i 7 §. Signal-skyddsverksamheten bedrivs, t.ex. genom avlyssning, rutinmässigt och inte alltid efter föregående misstanke om säkerhetshotande verksamhet.

I *andra stycket* föreskrivs att uppgifter om att en person kan antas ha samband med säkerhetshotande verksamhet skall försees med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Detta innebär att i förekommande fall skall en särskild upplysning lämnas om vilken trovärdighet som tillmäts t.ex. den som lämnat ett tips till säkerhetstjänsten. Om möjligt skall också anges hur korrekt uppgiften är, t.ex. om det är en obekräftad gissning eller ett belagt faktum.

När uppgifter behandlas i den militära säkerhetstjänsten är det av integritetsskäl viktigt att man särskiljer olika typer av uppgifter. Särskilt viktigt är att det inte uppstår missuppfattningar om i fall någon är misstänkt för att faktiskt utöva eller förbereda säkerhetshotande verksamhet eller inte. I *tredje stycket* anges att om

det inte klart framgår av sammanhanget att de uppgifter som behandlas om en person inte har som grund att personen är misstänkt för att bedriva säkerhetshotande verksamhet, skall särskild upplysning om detta förhållande göras i anslutning till personuppgifterna. Utgångspunkten är att särskilda upplysningar inte behövs när det av sammanhanget inte kan uppstå några tvivel om varför uppgifterna i fråga behandlas och det därför inte föreligger risk för att någon av misstag kan uppfattas som misstänkt för att bedriva säkerhetshotande verksamhet.

(Se *avsnitt 8.2.4*)

8 §

Enligt 13 § personuppgiftslagen är det som huvudregel förbjudet att behandla känsliga personuppgifter utan den enskildes samtycke. Om sådana uppgifter måste behandlas i offentlig verksamhet utan samtycke, och utan att något av undantagen från förbudet är tillämpligt, behövs det särskilda och avvikande bestämmelser för i vilka fall det får göras. Bestämmelserna i 8 § första och andra styckena överensstämmer med de i dag gällande bestämmelserna för Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten, se 4 § förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt.

I *första stycket* anges att känsliga personuppgifter inte får 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. Det innebär t.ex. att det inte är tillåtet att i underrättelseverksamheten föra register över, eller på annat sätt göra anteckningar om, enskilda personer enbart på den grunden att de tillhör en viss etnisk grupp.

Av *andra stycket* framgår att om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter när det är nödvändigt för syftet med behandlingen. Om det är nödvändigt för handläggningen av ärendet får de övriga uppgifterna i ärendet kompletteras med känsliga personuppgifter. Om Försvarsmakten i den militära säkerhetstjänsten får ett tips om att en viss person kan komma att bedriva säkerhetshotande verksamhet av något slag får naturligtvis anteckningar göras som kan underlätta identifiering av denna person, t.ex. uppgifter om fysiska kännetecken eller etniskt ursprung m.m. På samma sätt är det i försvarsunderrättelseverksamheten tillåtet att anteckna känsliga

personuppgifter om personer som på saklig grund är av intresse för verksamheten, under förutsättning att de känsliga uppgifterna är nödvändiga för att få fram den fullständiga underrättelseinformationen som behövs.

Bestämmelserna om känsliga personuppgifter gäller även vid behandling av uppgifter i Försvarmaktens databaser enligt 2 kap. (Se avsnitt 8.2.5)

9 §

Enligt bestämmelsen får personuppgifter lämnas ut till andra länder om sekretess inte hindrar det och det behövs för att Försvarmakten skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Uppgifter får också överföras till tredje land om det av annan anledning är nödvändigt med hänsyn till de ändamål för vilka uppgifter behandlas enligt lagen. Paragrafen är ägnad att uppfylla de krav på nationell lagstiftning som dataskyddskonventionen ställer när det gäller överföring av personuppgifter till andra länder. Huruvida ett utlämnade skall ske eller inte måste i sin helhet avgöras efter en sekretessprövning och försvars- och säkerhetspolitiska överväganden.

(Se avsnitt 8.2.6)

2 kap. Försvarmaktens databaser

1 §

I paragrafen anges att det skall finnas ett antal databaser i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten. Begreppet databas är juridiskt och inte tekniskt. Informationsdatabasen och underrättelse- och säkerhetsdatabasen är med andra ord rättsliga samlingsnamn på en eller flera gemensamma databaser eller register. I korthet kan en databas beskrivas som uppgiftssamlingar som med hjälp av automatiserad behandling används gemensamt i verksamheten. Uppgifterna har hämtats in i den militära underrättelse- och säkerhetstjänsten och har i databaserna gjorts gemensamt tillgängliga för olika handläggare inom organisationen med den begränsning som följer av befattningshavarens behörighet. Utanför databaserna faller däremot uppgifter i t.ex. e-post, ordbehandlingsdokument och tillfälliga register, som lagras på en hårddisk eller i en server på sådant sätt att de inte är allmänt tillgängliga inom Försvarmakten, utan åtkomliga endast för den person – eller ett fåtal personer i en

begränsad grupp – som tar emot e-postmeddelandet, upprättar dokumentet eller använder sig av det tillfälliga registret m.m.
(*Se avsnitt 8.3.1*)

2 §

I informationsdatabasen får Försvarsmakten samla information som hämtats in från öppna källor, såsom tidskrifter, litteratur och Internet m.m. för att underlätta tillgängligheten till sådan information i verksamheten. I övrigt får uppgifterna endast behandlas genom att föras över till underrättelse- och säkerhetsdatabasen.

(*Se avsnitt 8.3.3*)

3–4 §§

I underrättelse- och säkerhetsdatabasen skall i första hand samlas sådan information som samlats in från andra än öppna källor, dvs. hemliga och kvalificerat hemliga uppgifter. Underrättelse- och säkerhetsdatabasen är ett samlingsnamn för flera av de olika tekniska system som används i verksamheten för att behandla hemliga uppgifter för ändamålen försvarsunderrättelseverksamhet och militär säkerhetstjänst, t.ex. IS UNDSÄK, BANIO och MINSK.

I databasen får också behandlas uppgifter som överförts från informationsdatabasen av den anledningen att uppgifterna ansetts vara av intresse i den militära underrättelse- och säkerhetstjänsten. Information som lagras i underrättelse- och säkerhetsdatabasen får behandlas för att underlätta sökning efter uppgifter som samlats in från såväl öppna som hemliga källor. I databasen får vidare analys och bearbetning av inhämtat underrättelsematerial ske och färdiga underrättelserapporter lagras och delges inom systemet.

(*Se avsnitt 8.3.3*)

5 §

Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten är av sådan art att det inte är möjligt att i detalj reglera vilka uppgifter som får behandlas i verksamheterna. En noggrann reglering av vilka uppgifter som får behandlas måste också av naturliga skäl vara hemlig. I paragrafen bemyndigas regeringen, eller den myndighet som regeringen bestämmer, att meddela närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i databaserna. I den till lagen föreslagna förordningen finns bestämmelser om vilka uppgifter som får behandlas.

I 1 kap. 7 § finns vissa bestämmelser om innehåll som gäller för uppgifter som behandlas i den militära säkerhetstjänsten, vilka även gäller för den behandling som sker i Försvarsmaktens databaser.

(Se avsnitt 8.3.4)

6 §

I paragrafen förtydligas bestämmelsen i 1 kap. 8 § som reglerar användningen av känsliga personuppgifter och som redan den innebär en begränsning av möjligheten att använda känsliga personuppgifter som sökord. Bestämmelserna i förevarande paragraf innebär att sökning i databaserna inte får ske uteslutande med känsliga personuppgifter som grund för sökningen. Känsliga personuppgifter får endast användas som komplement när det finns ett annat för verksamheten berättigat skäl att sökningen sker. Bestämmelserna utesluter inte att känsliga personuppgifter kan användas ensamma vid sökning. De känsliga personuppgifterna får dock inte utgöra det enda ändamålet med sökningen.

(Se avsnitt 8.3.5)

7 §

Vilka som får ha direktåtkomst till Försvarsmaktens databaser bestäms av regeringen i förordning eller beslut. Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

(Se avsnitt 8.3.6)

3 kap. Enskildas rättigheter

1 §

Paragrafen innehåller bestämmelser om Försvarsmaktens skyldighet att informera den registrerade om att dennes personuppgifter är föremål för behandling. Av 23 § personuppgiftslagen framgår att den personuppgiftsansvarige självmant skall informera en enskild om behandling av uppgifter som samlas in från den enskilde själv. Den information som skall lämnas är enligt 25 § samma lag uppgift om den personuppgiftsansvariges identitet, ändamålen med behandlingen samt övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter. Information behöver dock inte lämnas om sådant som den registrerade redan känner till.

Information skall också enligt 26 § personuppgiftslagen lämnas på begäran av den registrerade. Om uppgifter behandlas skall

information lämnas om vilka uppgifter det rör sig om, varifrån uppgifterna hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut. Information behöver dock inte lämnas om personuppgifter i löpande text som inte har fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande, under förutsättning att uppgifterna inte har lämnats ut till tredje man.

Rätten till information gäller enligt 27 § personuppgiftslagen inte om det i lag eller annan författning eller i beslut som har meddelats med stöd av författning särskilt har föreskrivits att uppgifter inte får lämnas ut till den registrerade.

(Se avsnitt 8.4.1)

2 §

Bestämmelser om rättelse och skadestånd finns i 28 § respektive 48 § personuppgiftslagen och gäller vid behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten. Rätten till skadestånd avser de särskilda regler som gäller enligt personuppgiftslagen och omfattar därför endast levande fysiska personer, men det utesluter självfallet inte att även juridiska personer kan ha rätt till ersättning enligt de allmänna skadeståndsrättsliga principer som gäller vid skada som enskilda lider till följd av offentlig verksamhet.

(Se avsnitt 8.4.2)

3 §

De flesta beslut som fattas i Försvarmaktens verksamhet och som gäller behandling av personuppgifter enligt denna lag är interna eller administrativa och berör inte direkt enskildas intressen. Administrativa beslut fattas t.ex. om Försvarmakten beslutar att inom en viss databas inrätta särskilda register. Enskilda berörs dock direkt av myndighetens beslut om information och rättelse efter begäran. Sådana beslut är därför överklagbara. Talan mot beslut om information och rättelse förs i den normalt gällande ordningen i fråga om förvaltningsbeslut, nämligen till allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

(Se avsnitt 8.4.3)

4 §

Bestämmelserna om enskildas rätt till information gäller inte om sekretess är föreskriven för uppgifterna. Inom den militära

underrättelse- och säkerhetstjänsten gäller en omfattande sekretess vilket innebär att sådan information till den registrerade som avses i personuppgiftslagen i stort sett aldrig kommer att lämnas. Härigenom förts enskilda i praktiken även sin möjlighet att begära rättelse. Mot bakgrund härav skall en särskild myndighet ges i uppdrag att granska att behandlingen av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten sker i enlighet med bestämmelserna i denna lag. Granskningen skall således utgöra en kompensation för att enskilda, på grund av den sekretess som gäller i verksamheten, inte kan utnyttja den möjlighet till skydd för den personliga integriteten som lagens regler om information och rättelse m.m. ger.

Uppgiften att granska Försvarmaktens behandling av personuppgifter motsvarar vad som i dag gäller för Registernämnden inom polisens område. Detta innebär bl.a. att uppgiften inte förta det övergripande tillsynsansvar som åligger Datainspektionen enligt personuppgiftslagen. Den granskning som skall utföras enligt 4 § är en extra integritetsskyddskontroll som, utöver Datainspektionens tillsyn, skall skydda de registrerade mot otillbörligt intrång i den personliga integriteten. Försvarets underrättelsenämnd skall emellertid inte vara involverad i någon löpande ärendehantering hos Försvarmakten, och enskild skall inte kunna vända sig till nämnden med begäran om utlämnande av handlingar.

(Se avsnitt 8.5)

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

1 kap. Allmänna bestämmelser

1 §

Enligt *första stycket* skall lagen, liksom personuppgiftslagen, tillämpas på all behandling av personuppgifter som är helt eller delvis automatiserad samt viss strukturerad manuell behandling. Med personuppgifter avses detsamma som i personuppgiftslagen, nämligen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Begränsningen till underrättelseverksamhet innebär en avgränsning mot Försvarets radioanstalts övriga verksamheter. Vad som är underrättelseverksamhet legaldefinieras inte, men ledning kan

hämtas i 5 § om för vilka ändamål uppgifter får behandlas. Utanför lagens tillämpningsområde faller även behandling av personuppgifter i samband med de interna och administrativa åtgärder som kan förekomma i Försvarets radioanstalts verksamhet. För behandling av uppgifter som rör sådana frågor, t.ex. i personal- och löneregister, gäller i stället personuppgiftslagen.

Enligt *andra stycket* skall bestämmelserna om personuppgiftsansvar, ändamål samt de bestämmelser som gäller myndighetens databaser, tillämpas också på juridiska personer.

Bestämmelserna i 1 kap. är generella och gäller, om inte annat sägs, för all behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet, oavsett om det gäller e-post, enskilda tjänstemäns promemorior som upprättas i ordbehandlingsprogram, mindre register som används tillfälligt i underrättelseprojekt eller större register och datorsystem som används gemensamt i verksamheterna.

I *tredje stycket* upplyses om att det i 2 kap. finns särskilda bestämmelser för behandling av personuppgifter i Försvarets radioanstalts databaser.

(*Se avsnitt 8.2.1*)

2 §

Lagen gäller i stället för personuppgiftslagen (1998:204). I de fall bestämmelser i personuppgiftslagen är tillämpliga även på behandling i Försvarets radioanstalts underrättelseverksamhet anges det särskilt.

(*Se avsnitt 8.2.2*)

3 §

I paragrafen anges vilka bestämmelser i personuppgiftslagen som skall vara tillämpliga även vid behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet. De angivna bestämmelserna är alltså inte tillämpliga på behandling av uppgifter om juridiska personer.

(*Se avsnitt 8.2.2*)

4 §

Försvarets radioanstalt är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför. Personuppgiftsansvaret gäller även vid underlåtenhet att utföra en behandling som åligger Försvarets radioanstalt. Med personuppgiftsansvaret följer en rad skyldigheter. Den personuppgiftsansvarige skall bl.a. se till

att behandlingen av uppgifter sker på ett korrekt och säkert sätt samt att information lämnas till den registrerade.

Försvarets radioanstalt har även ansvar för uppgifter om juridiska personer, dvs. sådant som inte utgör personuppgifter. Ansvaret innebär motsvarande skyldigheter som personuppgiftsansvaret i fråga om de krav som lagen ställer på behandling av uppgifter om juridiska personer, t.ex. att uppgifterna endast får behandlas för tillåtna ändamål. Även ansvaret för att de krav som ställs upp i lagens 2 kap. för behandling av uppgifter i myndighetens databaser uppfylls, gäller för uppgifter om juridiska personer. Däremot är bestämmelserna i 3 kap. om enskildas rättigheter inte tillämpliga, vilket t.ex. innebär att Försvarets radioanstalts ansvar gentemot juridiska personer inte omfattar skyldighet att lämna information eller rätta uppgifter enligt personuppgiftslagen.

(Se avsnitt 8.2.3)

5 §

Paragrafen anger de ändamål för vilka uppgifter får användas – dvs. samlas in, registreras, lämnas ut och i övrigt behandlas – i Försvarets radioanstalts underrättelseverksamhet. Bestämmelsen tillämpas på uppgifter om såväl fysiska som juridiska personer. Försvarets radioanstalts underrättelseverksamhet bedrivs i huvudsak genom signalspaning.

Enligt lagen (2000:130) om försvarsunderrättelseverksamhet och den anslutande förordningen (2000:131) åligger det Försvarets radioanstalt att bedriva försvarsunderrättelseverksamhet för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Försvarsunderrättelseverksamhet består av inhämtning, bearbetning och analys samt delgivning av information. Härigenom utarbetas hotbildsanalyser och underrättelsebedömningar som delges främst Regeringskansliet och Försvarsmakten. Det är regeringen som bestämmer den närmare inriktningen av försvarsunderrättelseverksamheten.

Enligt *första stycket punkten 1* får uppgifter behandlas för säkerhetspolitiska och militärstrategiska bedömningar. Försvarsunderrättelseverksamheten skall identifiera och redovisa eller ge förvarning om sådana förändringar i omvärldsläget att detta kan ligga till grund för politiska beslut om totalförsvarets anpassning på kort eller lång sikt. Totalförsvaret är den verksamhet som behövs för att förbereda Sverige för krig och består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar), se 1 § lagen (1992:1403) om totalförsvaret och höjd beredskap.

Enligt *första stycket punkten 2* får uppgifter behandlas vid Sveriges deltagande vid internationella fredsbevarande och humanitära insatser, samt för att stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället. Det gäller att kunna förutse konflikter samt bearbeta inhämtat material och delge bedömningar om säkerhetspolitiska och militära förhållanden. Det kan också röra sig om att medverka med information och analys i fråga om sådant som t.ex. internationell terrorism och gränsöverskridande miljöhot.

Med *första stycket punkten 3* avses personlig information om t.ex. militär personal, politiker eller andra viktiga befattningshavare. Sådana uppgifter är nödvändiga att behandla för att informationsunderlaget till stöd för svensk utrikes-, försvars- och säkerhetspolitik skall bli komplett.

I *andra stycket* anges Försvarets radioanstalts uppgifter enligt 1–3 §§ förordningen (1994:714) med instruktion för Försvarets radioanstalt. Härav framgår att Försvarets radioanstalt inte enbart bedriver militärt inriktad underrättelseverksamhet utan även har andra uppgifter, bl.a. att med sin tekniska expertis lämna stöd för annan myndighetsverksamhet än sådan som rör yttre hot.

(Se avsnitt 8.2.4)

6 §

Enligt 13 § personuppgiftslagen är det som huvudregel förbjudet att behandla känsliga personuppgifter utan den enskildes samtycke. Om sådana uppgifter måste behandlas i offentlig verksamhet utan samtycke, och utan att något av undantagen från förbudet är tillämpligt, behövs det särskilda och avvikande bestämmelser för i vilka fall det får göras. Bestämmelserna i 6 § första och andra styckena överensstämmer med de i dag gällande bestämmelserna för Försvarets radioanstalts underrättelseverksamhet, se 4 § förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt.

I *första stycket* anges att känsliga personuppgifter inte får 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. Det innebär t.ex. att det inte är tillåtet att i underrättelseverksamhet föra register över, eller på annat sätt göra anteckningar om, enskilda personer enbart på den grunden att de tillhör en viss etnisk grupp.

Av *andra stycket* framgår att om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter när det är nödvändigt för syftet med behandlingen. Om det är nödvändigt för handläggningen av ärendet får de övriga uppgifterna i ärendet kompletteras med känsliga personuppgifter. Det är i Försvarets radioanstalts underrättelseverksamhet tillåtet att anteckna känsliga personuppgifter om personer som på saklig grund är av intresse för verksamheten, under förutsättning att de känsliga uppgifterna är nödvändiga för att få fram den fullständiga underrättelseinformation som behövs.

Bestämmelserna om känsliga personuppgifter gäller även vid behandling av uppgifter i Försvarets radioanstalts databaser enligt 2 kap.

(*Se avsnitt 8.2.5*)

7 §

Enligt bestämmelsen får personuppgifter 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. Uppgifter får också överföras till tredje land om det av annan anledning är nödvändigt med hänsyn till de ändamål för vilka uppgifter behandlas enligt lagen. Paragrafen är ägnad att uppfylla de krav på nationell lagstiftning som dataskyddskonventionen ställer när det gäller överföring av personuppgifter till andra länder. Huruvida ett utlämnade skall ske eller inte måste i sin helhet avgöras efter en sekretessprövning och försvars- och säkerhetspolitiska överväganden.

(*Se avsnitt 8.2.6*)

2 kap. Försvarets radioanstalts databaser

1 §

I paragrafen anges att det skall finnas ett antal databaser i Försvarets radioanstalts underrättelseverksamhet. Begreppet databas är juridiskt och inte tekniskt. I korthet kan en databas beskrivas som uppgiftssamlingar som med hjälp av automatiserad behandling används gemensamt i verksamheten. Uppgifterna har hämtats in i Försvarets radioanstalts underrättelseverksamhet och har i databaserna gjorts gemensamt tillgängliga för olika handläggare inom organisationen med den begränsning som följer av befattningshavarens behörighet. Utanför databaserna faller däremot uppgifter i

t.ex. e-post, ordbehandlingsdokument och tillfälliga register, som lagras på en hårddisk eller i en server på sådant sätt att de inte är allmänt tillgängliga inom Försvarets radioanstalt, utan åtkomliga endast för den person – eller ett fåtal personer – i en begränsad grupp – som tar emot e-postmeddelandet, upprättar dokumentet eller använder sig av det tillfälliga registret m.m.

(Se avsnitt 8.3.1)

2 §

I urvalsdatan skall de uppgifter behandlas som används för planering och inriktning av underrättelseverksamheten, på såväl lång som kort sikt. I databasen får behandlas de sökord i form av olika personuppgifter, t.ex. personnummer och namn, som används i underrättelseverksamheten vid sökning genom signalspaning och i öppna källor. Spaning sker även efter vissa tekniska parametrar, vilka även de kan återfinnas i urvalsdatan. Med parametrar avses såväl manuella som automatiska frekvenser, e-postadresser och telefonnummer.

(Se avsnitt 8.3.2)

3 §

I källdatan skall all information som Försvarets radioanstalt hämtar in genom signalspaning samlas. I databasen samlas obearbetad information som endast är ”en spegling” av förekommande signaler samt den signalspaningsinformation som inhämtats med hjälp av särskilt utvalda sökkriterier. Det inhämtade materialet kan vara såväl krypterat som avfattet på ett främmande språk.

Uppgifter som lagras i databasen får behandlas i den för att underlätta sökning efter information. I övrigt får uppgifterna endast behandlas genom att de förs över till analysdatan.

(Se avsnitt 8.3.2)

4 §

I databasen för öppna källor får Försvarets radioanstalt samla information som hämtats in på annat sätt än genom signalspaning. Sådan insamling sker t.ex. genom prenumeration på utländska tidningar, sökning efter information på Internet eller helt enkelt genom riktad inhämtning av uppgifter från olika webbsidor. Uppgifter som lagras i databasen får behandlas för att underlätta sökning efter information. I övrigt får uppgifterna endast behandlas genom att de förs över till analysdatan.

(Se avsnitt 8.3.2)

5 §

I analysdatabasen får de uppgifter behandlas som överförts från källdatabasen och databasen för öppna källor. Även annan för underrättelseverksamheten nödvändig information får behandlas i databasen. I databasen sker analys och annan bearbetning, såsom dekryptering och översättning, av den information som Försvarets radioanstalt hämtat in genom signalspaning och från öppna källor. I analysdatabasen får den information som undergår analys och bearbetning lagras fram till dess den färdigställs till underrättelse-rapporter och lagras i rapportdatabasen.

(Se avsnitt 8.3.2)

6 §

Rapportdatabasen får endast innehålla Försvarets radioanstalts färdiga underrättelserapporter som skall delges uppdragsgivarna. I rapporterna finns de underrättelser som framtagits genom analys och bearbetning i analysdatabasen.

(Se avsnitt 8.3.2)

7 §

Försvarets radioanstalts underrättelseverksamhet är av sådan art att det inte är möjligt att i detalj reglera vilka uppgifter som får behandlas i verksamheten. En noggrann reglering av vilka uppgifter som får behandlas måste också av naturliga skäl vara hemlig. I paragrafen bemyndigas regeringen, eller den myndighet som regeringen bestämmer, att meddela närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i databaserna. I den till lagen föreslagna förordningen finns bestämmelser om vilka uppgifter som får behandlas.

(Se avsnitt 8.3.4)

8 §

I paragrafen förtydligas bestämmelsen i 1 kap. 6 § som reglerar användningen av känsliga personuppgifter och som redan den innebär en begränsning av möjligheten att använda känsliga personuppgifter som sökord. Bestämmelserna i förevarande paragraf innebär att sökning i databaserna inte får ske uteslutande med känsliga personuppgifter som grund för sökningen. Känsliga personuppgifter får endast användas som komplement när det finns ett annat för verksamheten berättigat skäl att sökningen sker. Bestämmelserna utesluter inte att känsliga personuppgifter kan

användas ensamma vid sökning. De känsliga personuppgifterna får dock inte utgöra det enda ändamålet med sökningen.

(Se avsnitt 8.3.5)

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.

(Se avsnitt 8.3.6)

3 kap. Enskildas rättigheter m.m.

1 §

Paragrafen innehåller bestämmelser om Försvarets radioanstalts skyldighet att informera den registrerade om att dennes personuppgifter är föremål för behandling. Av 23 § personuppgiftslagen framgår att den personuppgiftsansvarige själv skall informera en enskild om behandling av uppgifter som samlas in från den enskilde själv. Den information som skall lämnas är enligt 25 § samma lag uppgift om den personuppgiftsansvariges identitet, ändamålen med behandlingen samt övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter. Information behöver dock inte lämnas om sådant som den registrerade redan känner till.

Information skall också enligt 26 § personuppgiftslagen lämnas på begäran av den registrerade. Om uppgifter behandlas skall information lämnas om vilka uppgifter det rör sig om, varifrån uppgifterna hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut. Information behöver dock inte lämnas om personuppgifter i löpande text som inte har fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande, under förutsättning att uppgifterna inte har lämnats ut till tredje man.

Rätten till information gäller enligt 27 § personuppgiftslagen inte om det i lag eller annan författning eller i beslut som har meddelats med stöd av författning särskilt har föreskrivits att uppgifter inte får lämnas ut till den registrerade.

(Se avsnitt 8.4.1)

2 §

Bestämmelser om rättelse och skadestånd finns i 28 § respektive 48 § personuppgiftslagen och gäller vid behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet. Rätten till skadestånd avser de särskilda regler som gäller enligt personuppgiftslagen och omfattar därför endast levande fysiska personer, men det utesluter självfallet inte att även juridiska personer kan ha rätt till ersättning enligt de allmänna skadeståndsrättsliga principer som gäller vid skada som enskilda lider till följd av offentlig verksamhet.

(Se avsnitt 8.4.2)

3 §

De flesta beslut som fattas i Försvarets radioanstalts verksamhet och som gäller behandling av personuppgifter enligt denna lag är interna eller administrativa och berör inte direkt enskildas intressen. Administrativa beslut fattas t.ex. om Försvarets radioanstalt beslutar att inom en viss databas inrätta särskilda register. Enskilda berörs dock direkt av myndighetens beslut om information och rättelse efter begäran. Sådana beslut är därför överklagbara. Talan mot beslut om information och rättelse förs i den normalt gällande ordningen i fråga om förvaltningsbeslut, nämligen till allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

(Se avsnitt 8.4.3)

4 §

Bestämmelserna om enskildas rätt till information gäller inte om sekretess är föreskriven för uppgifterna. Inom Försvarets radioanstalts underrättelseverksamhet gäller en omfattande sekretess vilket innebär att sådan information som avses i personuppgiftslagen i stort sett aldrig kommer att lämnas. Härigenom förtas enskilda i praktiken även sin möjlighet att begära rättelse. Mot bakgrund härav skall en särskild myndighet ges i uppdrag att granska att behandlingen av personuppgifter i Försvarets radioanstalts underrättelseverksamhet sker i enlighet med bestämmelserna i denna lag. Granskningen skall således utgöra en kompensation för att enskilda, på grund av den sekretess som gäller i verksamheten, inte kan utnyttja den möjlighet till skydd för den personliga integriteten som lagens regler om information och rättelse m.m. ger.

Uppgiften att granska Försvarets radioanstalts behandling av personuppgifter motsvarar vad som i dag gäller för Registernämnden inom polisens område. Detta innebär bl.a. att uppgiften inte förtar det övergripande tillsynsansvar som åligger Datainspektionen enligt personuppgiftslagen. Den granskning som skall utföras enligt 4 § är en extra integritetsskyddskontroll som, utöver Datainspektionens tillsyn, skall skydda de registrerade mot otillbörligt intrång i den personliga integriteten. Försvarets underrättelsenämnd skall emellertid inte vara involverad i någon löpande ärendehantering hos Försvarets radioanstalt, och enskild skall inte kunna vända sig till nämnden med begäran om utlämnande av handlingar.

(Se avsnitt 8.5)

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

9 kap. 27 §

I Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten gäller sekretess för uppgifter om enskildas personliga och ekonomiska förhållanden. Sekretess gäller om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men. För uppgifter som förekommer i allmänna handlingar kan sekretessen längst gälla i sjuttio år.

(Se avsnitt 10.1)

BILAGOR

Kommittédirektiv



Viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt

**Dir.
2002:13**

Beslut vid regeringssammanträde den 7 februari 2002.

Sammanfattning av uppdraget

En särskild utredare skall göra en översyn av regleringen av behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och i den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Utredaren skall därvid kartlägga behandlingen av personuppgifter och analysera behovet av särskilda bestämmelser. Utgångspunkten är att myndigheternas verksamhet skall kunna bedrivas effektivt med rationellt datorstöd samtidigt som nödvändig respekt visas för enskildas personliga integritet. Utredaren skall lämna förslag till en reglering i lag.

Uppdraget skall redovisas senast den 1 april 2003.

Nuvarande regler

För närvarande regleras Försvarmaktens och Försvarets radioanstalts personuppgiftsbehandling i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt och i personuppgiftslagen (1998:204). Förordningen trädde i kraft den 1 oktober 2001 och gäller utöver personuppgiftslagen, vilken trädde i kraft fullt ut för automatiserad

behandling av personuppgifter samma dag. Eftersom myndigheterna behandlar en stor mängd personuppgifter som dessutom kan vara av särskilt känslig natur bör behandlingen regleras särskilt i lag i stället för i förordning (se bet. 1990/91:KU11 s. 11 och bet. 1997/98:KU18 s. 43, jfr prop. 1990/91:60 s. 58 och 1997/98:44 s. 41).

Personuppgiftslagen gäller bl.a. för behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt. Lagen bygger på 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, kallat dataskyddsdirektivet (EGT nr L 281, 23/11/1995, s. 31–50, CELEX nr 1995L0046). Direktivet är inte tillämpligt på sådan behandling av personuppgifter som faller utanför gemenskapsrätten (exempelvis den som gäller allmän säkerhet, statens säkerhet eller statens verksamhet på straffrättens område). Den svenska personuppgiftslagen är dock generellt tillämplig och omfattar även sådana områden som faller utanför EG-rätten, i den mån det inte finns särreglering i andra författningar.

Utgångspunkten för personuppgiftslagen är att behandling av personuppgifter är tillåten bara i de fall och på de villkor lagen anger. Personuppgiftslagen innehåller vissa grundläggande krav på hur uppgifter får behandlas. Dessa krav innebär bl.a. att personuppgifter får behandlas endast för särskilda, uttryckligt angivna och berättigade ändamål. Enligt huvudregeln får behandling av uppgifter endast ske efter samtycke från den registrerade. Från huvudregeln finns det emellertid flera undantag, t.ex. om det är nödvändigt att behandla personuppgifter för att en arbetsuppgift av allmänt intresse skall kunna utföras eller för att den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet.

Förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt är tillämplig på den personuppgiftsbehandling som sker när myndigheterna, i förekommande fall, fullgör uppgifter enligt lagen (2000:130) om försvarsunderrättelseverksamhet, förordningen (2000:131) om försvarsunderrättelseverksamhet, säkerhetsskyddslagen (1996:627) och 1–3 §§ förordningen (1994:714) med instruktion för Försvarets radioanstalt.

Försvarsunderrättelseverksamhet och militär säkerhetstjänst

Försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Försvarsunderrättelseverksamheten syftar till att tillgodose behovet av tidig förvarning om hot mot landet så att beredskapshöjande åtgärder hinner vidtas samt att sörja för de underrättelsebehov som uppstår av Sveriges internationella verksamhet. Den militära säkerhetstjänsten i fred syftar till att tillgodose det långsiktiga säkerhetsskyddet inom Försvarsmakten.

Den vidgade synen på vad som innefattas i hot mot landets säkerhet medför att högre krav ställs på försvarsunderrättelsemyndigheterna beträffande samverkan och samordning med andra myndigheter. Den militära säkerhetstjänstens uppgift är att tillvarata de säkerhetsintressen som främst berör Försvarsmakten och att bl.a. biträda polisen i dess ansvar för rikets säkerhet. Säkerhetsintressena omfattar eller kan hänföras till personal, materiel, anläggningar, information samt planering och planer i vid bemärkelse. Säkerhetshotande verksamhet kan förekomma i form av underrättelseverksamhet, sabotage, subversiv verksamhet, terrorism och kriminalitet. Den militära säkerhetstjänsten omfattar säkerhetsunderrättelsetjänst och säkerhetsskyddstjänst. Vidare är signalskyddstjänsten en säkerhetsskyddsangelägenhet. Säkerhetsunderrättelsetjänstens uppgift är att klarlägga den säkerhetshotande verksamhetens omfattning, inriktning samt medel och metoder. Säkerhetsskyddet omfattar informations- och IT-säkerhet, tillträdesbegränsning, säkerhetsprövning, utbildning och kontroll. Samarbetet med andra länder och internationella organisationer är en naturlig del av försvarsunderrättelseverksamheten och säkerhetstjänsten. Ett utbyte av information är nödvändigt för att Sverige skall kunna få del av sådan information som landet behöver men som kräver resurser som saknas (jfr Regleringsbrev för budgetåret 2002 avseende myndigheter underställda Försvarsdepartementet s. 150–155).

Uppdraget

Utredaren skall göra en översyn av regleringen av Försvarmaktens och Försvarets radioanstalts behandling av personuppgifter. Uppdraget omfattar endast den personuppgiftsbehandling som sker när Försvarmakten fullgör uppgifter enligt lagen (2000:130) om försvarsunderrättelseverksamhet, förordningen (2000:131) om försvarsunderrättelseverksamhet och säkerhetsskyddslagen (1996:627) och i övrigt enligt vad som anges i 4 § 1–3 förordningen (2000:555) med instruktion för Försvarmakten samt när Försvarets radioanstalt fullgör uppgifter enligt lagen (2000:130) om försvarsunderrättelseverksamhet, förordningen (2000:131) om försvarsunderrättelseverksamhet och 1–3 §§ förordningen (1994:714) med instruktion för Försvarets radioanstalt.

Utredaren skall kartlägga behandlingen av personuppgifter såvitt nu är i fråga och analysera behovet av särskilda bestämmelser för myndigheternas behandling av personuppgifter samt lämna förslag till sådana bestämmelser i lag. Utredaren skall därvid granska frågor som rör användning, inhämtande, utlämnande, gallring, arkivering och tillsyn. Rent allmänt har utredaren stor frihet att ta upp andra frågor som anknyter till detta område och där så bedöms vara angeläget lämna förslag på lösningar. I arbetet skall det internationella inslaget i myndigheternas verksamheter beaktas.

Arbetet skall bedrivas med utgångspunkten att myndigheternas verksamhet skall kunna bedrivas effektivt med rationellt datorstöd samtidigt som nödvändig respekt visas för enskildas personliga integritet.

Enligt regeringens mening bör särlagstiftning gälla utöver personuppgiftslagen och begränsas till att avse frågor som är specifika för de verksamheter som omfattas av lagstiftningen.

Uppdragets genomförande

Utredaren skall samråda med Försvarmakten, Försvarets radioanstalt, Försvarets underrättelsenämnd, Rikspolisstyrelsen (SÄPO), Datainspektionen och Riksarkivet.

Utredaren bör även samråda med den särskilda utredare som är tillsatt för att göra en översyn av Försvarets radioanstalt.

Redovisning av uppdraget

Uppdraget skall redovisas senast den 1 april 2003.

(Försvarsdepartementet)

Försvarets radioanstalts underrättelseproduktion

