Rapport

Datainspektionens redovisning
av regeringsuppdraget
Fö2009/355/SUND
2010-12-06

Datainspektionen

1. Sammanfattning och bedömning

Denna rapport utgör Datainspektionens öppna redovisning av regeringsuppdraget Fö2009/355/SUND. Under delar av 2009 och 2010 har Datainspektionen, representerad av en projektgrupp, arbetat med att lösa de uppgifter som regeringen har önskat få genomlysta. I denna rapport redovisas resultatet av arbetet.

Den sammanfattande bedömningen är att frågor som har med personuppgiftsbehandling och personlig integritet att göra tas på allvar vid Försvarets radioanstalt (FRA) och att myndigheten har lagt ned mycket tid och resurser på att skapa rutiner och utbilda personalen på ett sådant sätt att risken för otillbörliga intrång i den personliga integriteten minimeras. Det intryck som Datainspektionen har fått under sin granskning är således på det hela taget positivt.

FRA är en organisation som i takt med teknikutvecklingen och utvecklingen i vår omvärld har kommit att stå inför nya utmaningar. Verksamheten är också bl.a. mot den bakgrunden reglerad på ett annat sätt än tidigare. På personuppgiftsområdet finns lagen (2007:259) om behandling av personuppgifter i FRA:s försvarsunderrättelse- och utvecklingsverksamhet (FRA-PuL) med anslutande förordning. Därutöver finns sedan den 1 januari 2009 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (LSF) med anslutande förordning. Lagen ändrades den 1 december 2009 (prop. 2008/09:201) i syfte att åstadkomma ett förstärkt integritetsskydd vid signalspaning. Datainspektionens uppdrag avser den personuppgiftsbehandling som tillämpningen av LSF föranleder vid FRA.

Den verksamhet som FRA:s signalspaning bl.a. har kommit att inrikta sig på avser idag i vissa delar helt nya miljöer och förhållanden, såväl tekniska som geografiska. Dessa omständigheter får även betydelse för den personuppgiftsbehandling som sker vid myndigheten. En mycket stor förändring är att FRA, efter införandet av LSF, får signalspana i kabel. I de nya signalmiljöerna är trafiken mer uppblandad än vad som gällde tidigare, då det främst var den militära eterburna trafiken som var föremål för signalspaning. Denna trafik kunde utan större problem hållas åtskild från "vanliga" människors kommunikation. Idag innebär tekniska lösningar som Internet och det globala nätet att personer med anknytning till de yttre hoten mot Sverige, t.ex. terrorverksamhet, i princip kommunicerar i samma nät som alla andra. Detta ställer högre krav än tidigare på att FRA med olika metoder kan välja ut just de signaler som är relevanta för de utrikes förhållanden och yttre hot som myndigheten har till uppgift att rapportera till sina uppdragsgivare. Att på motsvarande sätt selektera bort sådana signaler som är irrelevanta för verksamheten är mycket viktigt för att FRA ska kunna bedriva signalspaning på ett sätt som minimerar intrånget i den personliga integriteten.

Det bör understrykas att FRA, utöver den verksamhet som bedrivs i syfte att utveckla sina egna metoder, inte själva har några försvarsunderrättelsebehov. FRA utför således endast signalspaning på uppdrag av, i nuläget, regeringen, Regeringskansliet och Försvarsmakten. FRA ska delge underrättelser till berörda myndigheter enligt 2 § lagen (2000:130) om försvarsunderrättelseverksamhet. Det innebär att FRA har möjlighet att delge underrättelser med andra myndigheter än de som får agera uppdragsgivare i förhållande till FRA.

Datainspektionen har självklart tagit del av de påståenden och åsikter som ventilerades i den debatt som kringgärdade införandet av LSF. I denna rapport redovisas de iakttagelser som Datainspektionen har gjort under projektets gång och där det kan finnas anledning att ha synpunkter utifrån ett integritetsperspektiv kopplat till behandling av personuppgifter. Det ska dock redan nu understrykas att det inte gjorts några fynd som ger stöd för att det vid FRA pågår en omfattande personuppgiftsbehandling för syften som inte ligger inom ramen för försvarsunderrättelseverksamheten såsom den kommer till uttryck i den styrande lagstiftningen. Datainspektionen har således inte funnit att FRA behandlar personuppgifter i syfte att förse de brottsbekämpande myndigheterna med information om t.ex. fildelning eller liknande verksamhet. Inte heller har Datainspektionen gjort iakttagelser som tyder på att FRA behandlar personuppgifter i syfte att, i största allmänhet, kunna kartlägga Internetanvändande – eller kommunikation för syften som är otillåtna enligt LSF. Datainspektionen uppfattar att den personuppgiftsbehandling som bedrivs vid FRA görs för att utvinna underrättelser utifrån regeringens, Regeringskansliets och Försvarsmaktens behov inom ramen för landets säkerhets-, försvars- och utrikespolitik, dvs. för de syften som riksdag och regering har bestämt. Det innebär följaktligen att de svagheter och förbättringsområden som Datainspektionen har konstaterat avser den signalspaning med tillhörande personuppgiftsbehandling som FRA bedriver för dessa behov.

De särskilda integritetsproblem som kan uppstå i samband med den personuppgiftsbehandling som sker med anledning av FRA:s signalspaningsverksamhet enligt LSF, rör enligt Datainspektionen i huvudsak följande områden.

- **Trafikmängden i signalbärarna** - Datainspektionen gör bedömningen att mängden inhämtade signaler typiskt sett kommer att öka i och med att möjligheten till kabelinhämtning nu finns, vilket i sig bör leda till en potentiellt mer omfattande personuppgiftsbehandling vid FRA. Det beror på att inhämtningen sker i signalbärare som innehåller en större mängd signaler än t.ex. satellitstråk. Trafiken i kabelnätet är också mycket mer föränderlig till sin karaktär. Detta ställer högre krav på urval för att kunna säkerställa att endast den relevanta trafiken inhämtas och att veta var den trafiken uppträder, vilket i sin tur betonar

vikten av en effektiv utvecklingsverksamhet vid FRA. Det kan antas att den inhämtning som sker i kabel på sikt kommer att kunna begränsas på ett snävare sätt än vad som sker idag, i vart fall inom ramen för förvarsunderrättelseverksamheten.

- **Trafikdata** - Begreppet trafikdata förekom i den debatt som föregick antagandet av LSF, men finns inte som begrepp i lagstiftningen. Däremot talas om termen "råmaterial". Detta har lett till vissa oklarheter rörande vilken kategori som viss information ska hänföras till, vilket i sin tur kan få betydelse för tillämpningen av bl.a. gallringsregler. Inhämtning av trafikdata sker både i FRA:s utvecklingsverksamhet och i myndighetens försvarsunderrättelseverksamhet. Det huvudsakliga innehållet i FRA:s databas för trafikdata inhämtas inom ramen för försvarsunderrättelseverksamheten. Sökbegreppen vid inhämtning av trafikdata är mer generella än vid inhämtning av meddelanden och medför en omfattande behandling av personuppgifter hos FRA. Det innebär i sin tur att det finns en relativt hög sannolikhet för att de personer som kommunicerar i de signalbärare som FRA bedriver inhämtning mot, kommer att få uppgifter om sin kommunikation sparad hos FRA i form av trafikdata. Handläggarna vid FRA kan utföra sökningar i databasen för trafikdata inom ramen för de underrättelseärenden som de arbetar med. Bl.a. mot bakgrund av den omfattande mängd personuppgifter som behandlas i databasen för trafikdata anser Datainspektionen att FRA bör överväga tekniska sökbegränsningar i databasen och förstärka den införda loggуppföljningen. Syftet med dessa åtgärder ska vara att skydda de personuppgifter som finns i databasen mot otillbörliga intrång i den personliga integriteten.

- **S.k. inhemsk trafik** - När det gäller förbudet mot att inhämta s.k. inhemsk trafik, bör sådan trafik i första hand uteslutas från inhämtning genom användandet av automatiska processer som skiljer bort den otillåtna inhemska trafiken. I den uppgiftssamling som innehåller inhämtade meddelanden finns idag, såvitt avser satellitinhämtning, tillräckliga metoder för att urskilja inhemsk trafik. Avseende kabelinhämtning bedömer Datainspektionen dock att finns det behov av att förbättra metoderna för att över tiden urskilja sådan trafik med större noggrannhet. Även beträffande trafikdata kan inhemska signaler komma att inhämtas av FRA och bli föremål för vidare behandling i upp till ett år. FRA har infört mekanismer för att skilja bort sådana signaler, men det finns inga garantier för att sådana signaler aldrig inhämtas. Inhemsk trafik har också inhämtats av FRA. Det är därför viktigt att det finns fungerande rutiner för hur eventuell förekomst av sådan information ska hanteras.

- **Förstöringsskyldighet** – Upptagning eller uppteckning av uppgifter ska bl.a. förstöras om innehållet avser en viss fysisk person och bedöms sakna betydelse för sådan verksamhet som avses i 1 § LSF (7 § 1 p LSF). Datainspektionen har kunnat konstatera att en stor andel av de meddelanden som inhämtas av FRA tas bort kort tid efter inhämtningen, eftersom de bedöms vara irrelevanta. Inspektionen ifrågasätter om uppgifterna verkligen är att anse som analysmaterial eller om det i själva verket, i ett inledande skede, är fråga om råmaterial för vilket en absolut gallringsfrist på ett år gäller. I samband med att FRA:s analytiker ska ta bort ett meddelande från innehållsdatabasen, kan de använda sig av två metoder. Den ena metoden är särskilt utvecklad för att användas vid förekomst av förstöringspliktig information och den får mer omfattande effekter i FRA:s system; den andra metoden får inte lika ingripande effekter.

  Datainspektionen anser att det finns anledning för FRA att kontrollera, följa upp och dessutom utbilda handläggarna på ett sådant sätt att det säkerställs att samtliga meddelanden som omfattas av förstöringsskyldighet enligt i första hand 7 § 1 p LSF också förstörs på ett sådant sätt att informationen inte kan återskapas, dvs. att handläggarna använder sig av rätt metod. Det ska tilläggas att de två valbara metoderna, såsom de är utformade idag, inte innebär några större praktiska skillnader för personuppgiftsbehandlingen. När det gäller förstöringsskyldigheten enligt 7 § p 2-3 LSF råder det oklarheter kring den geografiska räckvidden av förstöringsskyldigheten, vilket kan få betydelse för den praktiska tillämpningen av bestämmelserna. Dessa oklarheter bör avhjälpas, t.ex. genom utbildning och handledning av den personal vid FRA som behandlar personuppgifter. Det är dessutom viktigt att FRA har rutiner som säkerställer att meddelanden som inhämtats inte blir föremål för vidare behandling, utan att det först har kontrollerats att meddelandena inte innehåller förstöringspliktig information. Sådana rutiner har nu införts vid FRA, vilket innebär ett ökat skydd vid behandling av personuppgifter.

- **Sökbegrepp** – Enligt 3 § 2 st LSF får sökbegrepp som är direkt hänförliga till en viss fysisk person användas endast om det är av synnerlig vikt för verksamheten. Detta indikerar enligt Datainspektionen en avsikt att sådana sökbegrepp inte skulle komma att användas som huvudregel. Datainspektionen har funnit att de sökbegrepp som FRA använder vid sin signalspaning i stor omfattning är direkt hänförliga till viss fysisk person. Eftersom bestämmelsen har betydelse för den behandling av personuppgifter som kommer att ske vid FRA i samband med signalspaning enligt LSF, vill Datainspektionen lyfta fram denna iakttagelse.

- **Känsliga personuppgifter** – Vid signalspaning kan s.k. känsliga personuppgifter komma att inhämtas. Sådana uppgifter får behandlas av FRA endast om vissa

förutsättningar är uppfyllda (1 kap. 11 § FRA-PuL). Det finns ingen teknisk funktion som säkerställer att den nödvändighetsbedömning som krävs görs och dokumenteras i FRA:s IT-system. En sådan funktion skulle vara av stort värde i syfte att säkerställa integritetsskyddet vid behandling av känsliga personuppgifter. FRA bör därför ta fram rutiner för den praktiska hanteringen av känsliga personuppgifter som säkerställer att de nödvändiga bedömningarna görs.

- **Underrättelse till enskild** – Den i 11 a § LSF beskrivna underrättelseskyldigheten vid användning av sökbegrepp som är direkt hänförliga till fysisk person har på grund av sekretess inte använts av FRA sedan bestämmelsen trädde ikraft. Värdet av denna underrättelseskyldighet som integritetsskyddande åtgärd kan därför ifrågasättas.

2. Uppdraget

Den 12 februari 2009 erhöll Datainspektionen regeringens uppdrag att under 2009 och 2010 ur ett integritetsskyddsperspektiv följa den personuppgiftsbehandling som tillämpningen av lagen (2008:717) om signalspaning i försvarsunderrättelseverksamheten (LSF) föranleder hos Försvarets radioanstalt (FRA). Inom ramen för uppdraget skulle Datainspektionen

- analysera vilka särskilda integritetsproblem som kan uppstå i samband med personuppgiftsbehandling i FRA:s signalspaningsverksamhet,
- utreda om de rutiner och riktlinjer som FRA tillämpar är tillräckliga för att hantera sådana problem, och
- bistå FRA vid utarbetandet av de ytterligare rutiner och riktlinjer som kan vara nödvändiga för att tillgodose integritetsskyddsbehovet vid personuppgiftsbehandling i signalspaningsverksamheten.

Uppdraget ingår som ett led i uppföljningen av LSF. Tyngdpunkten i uppföljningen ska ligga i det uppdrag som regeringen gett en parlamentarisk kommitté (Signalspaningskommittén, dir. 2009:10) i syfte att redovisa och bedöma konsekvenserna för enskildas integritet. Datainspektionens uppdrag ska komplettera kommitténs arbete i de delar där myndighetens specifika kompetens i fråga om integritetsskydd vid personuppgiftsbehandling särskilt bör tillvaratas. I uppdraget anges vidare att Datainspektionen ska utföra sitt arbete på ett sådant sätt att det inte påverkar den svenska försvarsunderrättelseverksamhetens förutsättningar att i dag och i framtiden arbeta för Sveriges bästa. I uppdraget anges dessutom att arbetet även i övrigt

ska bedrivas så att det inte skadar Sveriges förbindelser och samarbeten med andra länder.

Uppdraget återfinns i sin helhet som bilaga 1 till denna rapport.

3. Metod

Efter mottagande av uppdraget fattades vid inspektionen beslut om att bilda en projektgrupp som skulle lösa uppdraget. En projektgrupp bestående av tre jurister och två IT-säkerhetsspecialister, engagerades i projektet. Till projektet knöts en styrgrupp bestående av representanter från Datainspektionens myndighetsledning. Därefter analyserades uppdraget och en projektplan med tillhörande aktivitetslista togs fram. Projektplanen fastställdes under maj månad 2009. Därefter togs inledande kontakt med FRA och formerna för projektgruppens arbete diskuterades. Med hänsyn till den typ av information som projektet skulle ta del av, men även av praktiska skäl, bestämdes att arbetet med att lösa uppdraget skulle ske på plats vid FRA, på Lovön utanför Stockholm. Vid FRA har Datainspektionen disponerat ett eget rum med IT-utrustning och möjlighet att förvara hemligt material.

Efter etablering vid FRA har projektgruppens personal erhållit nödvändiga behörigheter för att kunna arbeta med det material som förekommer i FRA:s signalspaningsverksamhet.

Inledande kontakter har i ett tidigt skede också tagits med den dåvarande Signalspaningsnämnden (senare Försvarsunderrättelsedomstolen), dåvarande Försvarets underrättelsenämnd (FUN) (numera Statens inspektion för försvarsunderrättelseverksamheten (SIUN)) och med Signalspaningskommittén. Slutligen har kontakt även tagits med Integritetsskyddsrådet vid FRA (ISR). Under projektets gång har kontakt och samverkan framförallt förekommit med Signalspaningskommittén.

En stor del av arbetet under 2009 har gått åt till att få utbildning av FRA på området signalspaning och de metoder som myndigheten använder för att lösa sina uppgifter. Därutöver har Datainspektionen under 2009 även granskat FRA:s föreskrifter. Under arbetets gång har således samtliga relevanta föreskrifter, ett tiotal, granskats och skriftliga synpunkter har löpande lämnats till FRA för återkoppling och eventuella åtgärder. Från senare delen av 2009 och under 2010 har arbetet huvudsakligen varit inriktat på praktisk granskning av den personuppgiftsbehandling som FRA:s signalspaning enligt LSF ger upphov till.

Vidare har Datainspektionen tillsammans med Signalspaningskommitt61 haft ett tiotal sammankomster där FRA har gått igenom olika områden inom signalspaningen och där företrädare för FRA har svarat på frågor och närmare förklarat förhållanden som kommittén och Datainspektionen har anmält. På detta sätt har Datainspektionens projektgrupp erhållit de ytterligare kunskaper som behövts för att kunna lösa uppdraget. Inom ramen för uppdraget har Datainspektionen också haft vissa kontakter med SIUN och till viss del även ISR. Syftet med den samverkan har i huvudsak varit inriktat på erfarenhets- och kunskapsutbyte, samt på vissa uppdateringar och samordning.

Datainspektionen har även valt att granska enskilda ärenden hos FRA, utifrån de antaganden om tänkbara risker för den personliga integriteten som FRA:s signalspaning kan innebära såvitt avser behandling av personuppgifter, samt för att följa upp FRA:s rutiner och riktlinjer i den praktiska handläggningen vid myndigheten. En viktig del i ärendegranskningen har också varit att över tiden skapa en bild av med vilken precision som FRA:s inhämtningssystem klarar av att urskilja och välja ut för verksamheten relevanta och tillåtna signaler – en omständighet av central betydelse för den personuppgiftsbehandling som signalspaningen medför.

Dessutom har Datainspektionen riktat sin uppmärksamhet mot området IT-säkerhet och inom ramen för detta undersökt om de åtgärder som FRA vidtar är tillräckliga för att säkerställa ett tillräckligt skydd för de personuppgifter som myndigheten behandlar i sin verksamhet med anledning av tillämpningen av LSF.

Avslutande del av arbetet har ägnats åt att sammanställa den information som Datainspektionen har erhållit och de iakttagelser som har gjorts. Inspektionen har strävat efter att endast redovisa sådana slutsatser av sitt arbete som har betydelse för integritetsskyddet vid behandling av personuppgifter vid FRA. Vidare har inspektionen inte heller haft för avsikt att inkräkta på de andra tillsynsorganens verksamhet. Datainspektionen har dessutom inte i någon del granskat den verksamhet som sker vid Försvarsunderrättelsedomstolen eller i övrigt haft för avsikt att ha någon uppfattning om domstolens arbete.

För att på ett bra sätt kunna hantera och skydda den information och de kunskaper som projektmedlemmarna erhållit under arbetets gång, har inget material som tillförts projektet förts från FRA. Allt arbete har således skett på plats vid myndigheten. Inte heller har någon kommunikation avseende projektet, utöver rent administrativa meddelanden, befordrats över öppna kommunikationsnät. På detta sätt har projektet kunnat upprätthålla en egen hög signalskyddsnivå under arbetets genomförande.

4. Avgränsningar

Datainspektionens mål har varit att genomföra en så heltäckande genomlysning som möjligt av den personuppgiftsbehandling som LSF ger upphov till vid FRA. Det finns dock delar av verksamheten som inspektionen endast har granskat översiktligt. Till denna kategori hör främst den s.k. partnersamverkan, dvs. FRA:s samarbete med andra staters motsvarigheter.

Datainspektionen har inte heller närmare granskat sådan personuppgiftsbehandling som avser rent militär kommunikation, eftersom integritetsaspekterna där inte kan anses göra sig lika starkt gällande som för annan kommunikation.

En annan avgränsning avser granskningen av FRA:s signalspaning i kabel. Denna granskning har kommit att bli begränsad i vissa delar till följd av att FRA:s kabelinhämtning av olika skäl inte har kommit igång förrän mot slutet av projekttiden. Det är således först under projektets senare del som det överhuvudtaget har förekommit trafik från kabel i de enskilda ärenden som Datainspektionen har granskat. Det har dessutom rört sig om en i sammanhanget liten mängd trafik. Datainspektionens slutsatser beträffande kabelinhämtningen är således inte på samma sätt som avseende satellit- och annan eterburen inhämtning baserade på de bedömningar som inspektionen har kunnat göra utifrån egna observationer i den skarpa inhämtningen. Datainspektionen anser dock att de slutsatser som redovisas i rapporten och som avser signalspaning i kabel kan anses som tillförlitliga, bl.a. mot bakgrund av de likheter som ändå finns jämfört med satellitinhämtning. Det är dock viktigt att tillsynsorganens fortsatta verksamhet, som kommer att ske i en miljö med en bedömt betydligt högre förekomst av kabelinhämtat material och förmodat större trafikvolymer, följer upp de bedömningar och slutsatser som har dragits i dessa delar.

5. Förhållandet till FRA

Datainspektionen är tillsynsmyndighet avseende personuppgiftsbehandlingen vid FRA enligt lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA-PuL). Inspektionen är också tillsynsmyndighet avseende personuppgiftsbehandling i samhället i övrigt, dvs. även sådan behandling som sker hos t.ex. Försvarsmakten, de brottsbekämpande myndigheterna och i andra sammanhang. Datainspektionen utövar sin tillsyn med stöd av personuppgiftslagen (1998:204) och särskild lagstiftning, såsom FRA-PuL. En normal del av tillsynsverksamheten består av olika former av inspektioner på plats vid de berörda myndigheterna och övriga tillsynsobjekt. Tillsynsaktiviteterna kan initieras via

Datainspektionens egen planering och prioriteringar, men även efter tips och klagomål från allmänheten eller uppgifter som förekommer i massmedia.

Den tillsyn som Datainspektionen har bedrivit för att lösa det nu aktuella uppdraget har i väsentliga avseenden skilt sig från inspektionens ordinarie tillsynsverksamhet. För det första har den tagit stora personella resurser i anspråk och bedrivits under lång tid. Dessutom har den inledningsvis krävt att Datainspektionens personal har utbildats i den verksamhet som ska granskas, vilket normalt inte är fallet. Utbildningen har dessutom getts av det organ som ska granskas, dvs. av FRA. En annan aspekt som gör lösandet av regeringsuppdraget speciellt är att det har avsett en verksamhet som i princip helt och hållet ligger utanför allmänhetens insyn och som omfattas av stark sekretess. Det har ställt särskilda krav på hantering av information och arbetssätt. Datainspektionens projektgrupp har vidare varit beroende av att FRA har kunnat leverera den information som projektet har begärt och i övrigt vara tillgängliga med information och personal i takt med att nya behov har dykt upp. FRA har i denna del varit fullt behjälpliga och Datainspektionen har följaktligen fått erforderliga möjligheter att kunna ställa de frågor och granska de personuppgiftsbehandlingar som har begärts. Klimatet mellan Datainspektionen och FRA har också varit sådant att uppkomna frågeställningar löpande har kunnat hanteras. När det har bedömts lämpligt eller nödvändigt, har erforderliga åtgärder i princip genast kunnat vidtas från FRA:s sida. Uppdraget har således inneburit att FRA löpande under projekttiden beaktat flertalet av de synpunkter som Datainspektionen har lämnat avseende FRA:s personuppgiftsbehandling.

6. Ekonomi

För lösandet av uppdraget har Datainspektionen disponerat 1 500 TSEK, varav 1 000 TSEK att använda under 2009 och 500 TSEK under 2010. I maj 2009 rekvirerade Datainspektionen således 1 000 TSEK från FRA. I enlighet med instruktionerna i uppdraget lämnade Datainspektionen den 16 oktober 2009 en ekonomisk redovisning och prognos. I oktober 2009 hade Datainspektionen förbrukat ca. 350 TSEK av de dittills rekvirerade 1 000 TSEK.

I syfte att följa projektets kostnader har löpande kontroll gjorts mot det avräkningskonto som projektet haft vid Datainspektionen. Projektpersonalen har löpande redovisat sin nedlagda tid i projektet i Datainspektionens tidredovisningssystem. För lösande av uppdraget har slutligen kommit att användas ca 1 000 TSEK, dvs. två tredjedelar av de tilldelade 1 500 TSEK.

De förbrukade medlen har i princip uteslutande utgjorts av arbetad tid. En mindre del har avsett reskostnader. Några inköp av IT- eller säkerhetsutrustning, vilket inledningsvis planerades för, har inte varit nödvändigt. En närmare redovisning över det ekonomiska utfallet återfinns i bilaga 2.

7. Personlig integritet

I Datainspektionens uppdrag har legat att undersöka signalspaningens inverkan på den personliga integriteten vid behandling av personuppgifter. En utgångspunkt i detta arbete har varit att försvarsunderrättelseverksamheten är en viktig del i skyddet av riket och att signalspaning i eter och tråd utgör en betydelsefull del i denna verksamhet.

Vid diskussioner om hur den personliga integriteten ska skyddas är en återkommande fråga vad som egentligen avses med detta begrepp. Det kan direkt konstateras att begreppet är svårdefinierat. Det finns inte heller någon allmänt vedertagen definition av begreppet i svensk rätt, även om det har gjorts ett stort antal försök definiera det. För att signalspaningens effekter på den personliga integriteten ska kunna bedömas är det dock nödvändigt att i någon mån klargöra vad som avses med personlig integritet. I det följande lämnas därför en kortare beskrivning av vad som i olika sammanhang uttalats i denna fråga.'

7.1 Allmänt om personlig integritet

Integritet beskrivs ofta som en inre egenskap, som är olika hos olika individer. "Rätten att få vara i fred" är en vanlig tolkning. "Rätten att få sin personliga egenart och inre sfär respekterad och att inte utsättas för kränkande behandling" är en annan. Begreppet personlig integritet kan alltså sägas beteckna såväl relationen mellan olika individer, som — i fallet signalspaning — mellan staten och individen. I grunden handlar det om att fastställa de rättigheter och skyldigheter som råder mellan individer i olika situationer. Uppfattningen om hur långt den privata sfären sträcker sig kan naturligtvis variera kraftigt mellan olika individer. Räckvidden av den privata sfären är inte heller statisk, inte ens för den enskilda individen, utan kan förändras över tid beroende på den aktuella situationen.[2]

I svensk rätt saknas som ovan nämnts en entydig och allmänt vedertagen definition av begreppet personlig integritet. Samma ord — personlig integritet — används till exempel för att beteckna olika slags integritet, såväl kroppsliga som psykologiska aspekter av denna. Begreppet används också i olika sammanhang med delvis olika betydelser. Personlig integritet är inte heller det enda begrepp som förekommer. I

Europakonventionen talas t.ex. om skyddet för enskildas privatliv. Ett annat exempel är begreppet "privatlivets fred", som användes av 1966 års integritetsskyddskommitté. Här bör också nämnas den engelska termen "privacy", som även det kan översättas med "privatlivets fred" eller liknande.

Oavsett hur man väljer att avgränsa eller definiera begreppet personlig integritet, finns det ett behov av att ta hänsyn till de motstående intressen som aktualiseras vid behandling av personuppgifter. Personlig integritet är såsom framgår under avsnitt *8.1 Grundlagarna* nedan inte absolut utan relativ, dvs. den utgör en välgrundad och giltig rättighet som i det enskilda fallet kan sättas ur spel om det finns motstående intressen som bedöms väga tyngre. När den personuppgiftsbehandling som signalspaningen medför ska bedömas ur ett integritetsperspektiv handlar det därför i praktiken om att väga den nytta och effektivitet som signalspaningen innebär mot de möjliga och relevanta intrång i den personliga integriteten som uppstår till följd av åtgärden.

Utformandet av integritetsskyddet i svensk rätt har i praktiken inte utgått från en viss definition av begreppet integritet. Det har istället handlat om att förbjuda sådana företeelser som inte ansetts försvarbara med hänsyn till dels den skada de skulle innebära för den personliga integriteten, dels den skada som ett upprätthållande av integriteten skulle orsaka andra beaktansvärda intressen.

Ingrepp i den personliga integriteten kan vara allt från bagatellartade till ytterst kränkande för den berörda individen. Det finns därför anledning att skilja på sådana åtgärder som förvisso innebär ett intrång i enskildas personliga integritet, men som trots allt får anses acceptabla, och sådana otillbörliga intrång i den personliga integriteten som enskilda inte ska behöva tåla. Hur allvarligt ett intrång i den personliga integriteten bedöms vara beror i grunden på informationens innehåll och hantering. Omständigheter som spelar in vid bedömningen är bland annat informationens art, mängd, aktualitetsgrad, korrekthet, användning, lagring och metoder för insamling.[3]

7.2 Personlig integritet inom ramen för signalspaning – särskilda utmaningar och säraarter

FRA behandlar i sin försvarsunderrättelseverksamhet en mycket stor mängd personuppgifter som inhämtas genom signalspaning. I och med utvidgandet av signalspaning till att avse signaler i kabel, kommer inhämtningen att rikta sig mot helt nya miljöer och förhållanden där det inte bara finns sådan trafik som kan vara relevant för försvarsunderrättelseverksamheten, utan där trafiken huvudsakligen innefattar "vanliga" människors kommunikation, som är helt utan betydelse för sådan verksamhet. Detta ställer högre krav på FRA att ta fram metoder för att i största möjligaste

utsträckning endast välja ut sådana signaler som är relevanta och att därutöver förstöra sådan information som ändå har inhämtats men som saknar betydelse.

En annan utmaning för integritetsskyddet i samband med FRA:s personuppgiftsbehandling är att verksamheten, av naturliga skäl, är kringgärdad med stark sekretess. Möjligheterna för den enskilde att få kännedom om och insyn i den personuppgiftsbehandling som sker är därför starkt begränsade jämfört med vad som gäller för annan verksamhet. Detta ställer krav på att det finns andra skyddsåtgärder som kompenserar bristen på insyn, såsom en klar och tydlig lagstiftning och effektiva kontrollorgan som kan följa upp efterlevnaden av reglerna.

En särskild fråga i samband med FRA:s signalspaningsverksamhet är också i vilket skede som de inhämtade signalerna är av sådan art att de träffas av skyddsreglerna ifråga om behandling av personuppgifter. Det är viktigt att den lagstiftning som ska skydda den personliga integriteten i samband med personuppgiftsbehandling inte får den motsatta effekten, dvs. att den tvingar fram otillbörliga integritetsintrång som annars inte skulle finnas.

Att myndigheten aktivt efterforskar förekomsten av förstörelsepliktig information i systemen – och därmed i praktiken riskerar att ta del av särskilt skyddsvärd information som annars inte skulle ha upptäckts – innebär i sig ett integritetsintrång, som eventuellt inte står i rimlig proportion till vad som skulle vinnas med åtgärden. Ett annat exempel är förbudet mot att inhämta viss typ av kommunikation såsom grundlagsskyddade meddelanden till journalister etc. Detta skulle kunna anses ställa krav på att FRA har tillgång till uppgifter om alla de personer som tillhör en sådan yrkesgrupp eller personalkategori och samtliga teleadresser och motsvarande som är hänförliga till personen i fråga. Endast genom att lägga in sådana uppgifter som exkluderande sökbegrepp i urvalssystemen kan ett inhämtningsförbud efterlevas fullt ut. Många anser dock att en sådan metod skulle innebära ett oproportionerligt stort integritetsintrång i förhållande till vad som skulle vinnas med åtgärden (se bl.a. prop. 2008/09:201, sid. 80). Datainspektionen delar den uppfattningen.

8. Relevant lagstiftning

I fråga om FRA:s signalspaning aktualiseras en rad olika bestämmelser i diverse lagar och andra författningar som måste beaktas för att skyddet av den personliga integriteten ska kunna bedömas.

8.1 Grundlagarna m.m.

I grundlagarna finns flera olika bestämmelser som behandlar skyddet för den enskildes integritet gentemot det allmänna. Integritetskränkningar som sker till följd av enskildas handlande, t.ex. enskilda tjänstemän hos det allmänna, regleras istället genom bestämmelser i annan lag, t.ex. i brottsbalkens regler om tjänstefel.

En grundläggande bestämmelse om skydd för den enskildes personliga integritet finns i 1 kap. 2 § fjärde stycket regeringsformen (RF), som stadgar att det allmänna ska värna den enskildes privatliv och familjeliv. Bestämmelsen utgör en målsättning för den offentliga verksamheten. Målsättningen preciseras i 2 kap RF. Detta kapitel innehåller bestämmelser om grundläggande fri- och rättigheter i form av, för domstolar och myndigheter, rättsligt bindande föreskrifter som skyddar den personliga integriteten i förhållande till det allmänna. Enligt 2 kap. 3 § får ingen svensk medborgare utan samtycke antecknas i ett allmänt register enbart på grund av sin politiska åskådning. I andra stycket sägs att varje medborgare, i den utsträckning som närmare anges i lag, ska skyddas mot integritetskränkningar som kan uppkomma genom att uppgifter om honom registreras med hjälp av automatisk databehandling. Enligt 2 kap. 6 § RF första stycket är vidare varje medborgare gentemot det allmänna skyddad mot bl.a. hemlig avlyssning, upptagning av telefonsamtal eller annat förtroligt meddelande. Skyddet omfattar såväl hemlig avlyssning som sker samtidigt med ett samtal som upptagning av ett samtal för senare avlyssning (SOU 1998:46 s. 51).

Bestämmelsen i 2 kap. 6 § RF hör till de grundläggande fri- och rättigheter som inte är absoluta utan kan inskränkas genom lag (2 kap. 12 § RF). På den inskränkande lagstiftningen ställs flera krav, bl.a. att den endast får göras för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle. Begränsningen får inte heller gå utöver vad som är nödvändigt för detta ändamål och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning. Skyddet gäller för svenska medborgare. Utlänning som vistas i Sverige ska dock likställas med svenska medborgare om inte annat är föreskrivet (2 kap. 22 § andra stycket 3 RF).

I november 2010 fattade riksdagen beslut om ändringar i regeringsformen. Ändringarna består bl.a. i ett nytt andra stycke i 2 kap. 6 §. Enligt den nya bestämmelsen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Samtidigt upphävs bestämmelsen i 2 kap. 3 § andra stycket då den inte anses ge upphov till något individuellt rättighetsskydd för enskilda utan endast en skyldighet för lagstiftaren att i lag upprätta någon form av integritetsskydd ifråga om automatiserad behandling av personuppgifter (prop.

2009/10:80, sid. 173 D. Sådana bestämmelser finns t.ex. i personuppgiftslagen (1998:204) och lagen (2007:259) om behandling av personuppgifter i FRA:s försvarsunderrättelse- och utvecklingsverksamhet. Ändringarna i regeringsformen träder ikraft den 1 januari 2011.

Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) som antogs av Europarådet år 1950, gäller som svensk lag (SFS 1994:1219). Som svensk lag gäller även de tilläggsprotokoll som hör till konventionen. Enligt 2 kap. 23 § RF får lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden enligt EKMR. Enligt artikel 8.1 EKMR har var och en rätt till skydd för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Överföring av meddelanden med hjälp av telefon, telefax, radio och datorer omfattas av EKMR:s skydd. Det innebär ett ingrepp i skyddet för korrespondens när någon hindrar eller kontrollerar sådan kommunikation.

Precis som i RF finns det i EKMR bestämmelser som anges under vilka förutsättningar som skyddet i artikel 8.1 får inskränkas. En sådan inskränkning måste ske med stöd av lag och vara ägnad att tillgodose något av de i artikel 8.2 uppräknade allmänna eller enskilda intressena. Bland dessa intressen återfinns statens säkerhet, den allmänna säkerheten och förebyggande av oordning eller brott. Inskränkningen måste vidare vara nödvändig i ett demokratiskt samhälle för att tillgodose det aktuella intresset. Det innebär att det måste finnas ett angeläget samhälleligt behov av inskränkningen och att den måste stå i rimlig proportion till det syfte som ska tillgodoses genom ingreppet. Undantaget ska dessutom vara utformat med sådan precision att inskränkningen av rättigheten i rimlig utsträckning är förutsägbar. När det gäller inskränkningar som har med statens säkerhet att göra har det anförts att det finns en vidsträckt möjlighet att göra avvägningar på nationell nivå och att Europadomstolens kontroll därmed är mindre omfattande (se Danelius, Mänskliga rättigheter i europeisk praxis, 2002, s. 264). I domstolens praxis har slagits fast att hemlig teleavlyssning och hemlig teleövervakning utgör ett intrång i såväl privatliv som korrespondens men att de kan vara godtagbara om de är nödvändiga för att skydda den nationella säkerheten eller för att förhindra oordning eller brott.

Enligt artikel 13 EKMR ska var och en som anser sig ha fått sina fri- och rättigheter kränkta ha rätt till ett effektivt rättsmedel inför en nationell myndighet. Detta gäller även om kränkningen utförts av offentlig myndighet. Det krävs inte att prövningen görs av en domstol, utan även administrativa rättsmedel inklusive olika former av övervaknings- och kontrollåtgärder kan vara tillräckliga för att uppfylla kravet.

Utöver de nämnda bestämmelserna i RF och EKMR finns ett annat skydd för vissa typer av kommunikationer i yttrandefrihetsgrundlagen (YGL) och tryckfrihetsförordningen (TF). Härigenom skyddas den som vill uttrycka sig i tryckt skrift (1:1 TF) eller i

radioprogram, ljud- och bildupptagningar (1:2 YGL). Bestämmelserna ger inte bara en rätt att själv yttra sig utan också att meddela uppgifter och underrättelser till annan för offentliggörande. Denna meddelarfrihet garanteras ytterligare genom ett anonymitetsskydd som bl.a. innebär att journalister och andra (med vissa undantag) har tystnadsplikt beträffande vem som har lämnat meddelanden enligt 1:1 TF och 1:2 YGL. I TF och YGL förbjuds vidare det allmänna att efterforska vem som har lämnat uppgifter för publicering i de olika medierna eller, med undantag för de fall då åtal eller annat ingripande mot honom eller henne kan ske med stöd av grundlagarna (3:3, 4 TF och 2:3, 4 YGL).

8.2 Regler om integritetsskydd i samband med personuppgiftsbehandling

Ett område där det har ansetts finnas särskilda behov av integritetsskydd är vid behandling av personuppgifter på automatiserad väg i datorer eller manuellt i register. Bestämmelser till skydd för integritetskränkningar genom sådan behandling finns i personuppgiftslagen (1998:204), som grundar sig på ett EG-direktiv (95/46/EG av den 24 oktober 1995). Personuppgiftslagen omfattar i princip personuppgiftsbehandling på alla områden, även sådan behandling som rör allmän säkerhet, försvar, statens säkerhet och brottsbekämpning. På många områden finns dock särskilda regler som anger närmare förutsättningar för personuppgiftsbehandling på just det området. Sådana särskilda regler tar över personuppgiftslagens bestämmelser i motsvarande delar. I vissa fall utesluter särskild lag helt personuppgiftslagens tillämpning.

I 6 kap. lagen (2003:89) om elektronisk kommunikation finns särskilda regler om skydd för den enskildes integritet vid tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster m.m.

8.3 Lagstiftning om behandling av personuppgifter i FRA:s försvarsunderrättelse- och utvecklingsverksamhet

För behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet finns särskilda bestämmelser i lagen (2007:259) (FRA-PuL) med tillhörande förordning (2007:261) (FRA-PuF). FRA-PuL och FRA-PuF gäller istället för personuppgiftslagen. Enligt en särskild bestämmelse i FRA-PuF är Datainspektionen tillsynsmyndighet över den personuppgiftsbehandling som sker enligt lagen.

I FRA-PuL anges grundläggande krav som FRA ska iaktta vid behandlingen av personuppgifter. Därutöver anges att FRA får behandla personuppgifter i olika uppgiftssamlingar i sin försvarsunderrättelse- och utvecklingsverksamhet. I försvarsunderrättelseverksamheten får uppgifter om en person behandlas endast om

personen har anknytning till en preciserad inriktning och behandlingen är nödvändig för att fullfölja den inriktningen. Vidare får s.k. känsliga personuppgifter inte behandlas annat än som kompletterande information till personuppgifter som behandlas på annan grund och endast när det är absolut nödvändigt för syftet med behandlingen. Uppgifter får alltså inte behandlas om en person enbart på den grunden att personen är av viss etniskt ursprung, har viss politisk åsikt eller religiös uppfattning, är medlem i viss facklig organisation. Inte heller får uppgifter om en person behandlas enbart på grund av dennes hälsotillstånd eller sexualliv. Användning av sådana uppgifter som sökbegrepp får ske endast om det är absolut nödvändigt för syftet med behandlingen. I FRA-PuL finns också begränsningar ifråga om behandling av personnummer, som motsvarar personuppgiftslagens regler.

I en särskild bestämmelse (1 kap. 13 § FRA-PuL) anges att inhämtning av uppgifter genom signalspaning samt efterföljande lagring m.m. inte ska ses som oförenlig med de nyss nämnda bestämmelserna i det skede då det inte går att fastställa om informationen innehåller personuppgifter. Enligt Datainspektionen är det i de flesta fall då personuppgifter behandlas i signalspaningsverksamheten möjligt att omgående konstatera om en viss upptagning eller uppteckning innehåller personuppgifter, t.ex. ett telefonnummer eller en e-postadress.

De uppgiftssamlingar som får finnas hos FRA är, enligt FRA-PuF, uppgiftssamlingar för råmaterial, för analyser, för underrättelser samt för information om signalmiljö och för information om företeelser mot vilka signalspaningen inriktas. Uppgiftssamlingar för råmaterial ska gallras inom ett år (2 § FRA-PuF). Särskilda regler om gallring finns också för uppgiftssamlingarna med information om signalmiljön (5 § 2 st FRA-PuF) och företeelser mot vilka signalspaningen inriktas (6 § 2 st FRA-PuF). I övrigt gäller en generell gallringsregel i 6 kap. 1 § FRA-PuL, nämligen att personuppgifter ska gallras så snart de inte längre behövs för det ändamål för vilket de behandlas. Regeringen eller arkivmyndighet kan dock meddela föreskrifter om gallring vid viss tidpunkt eller att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål. Krigsarkivet beslutade i mars 2009 att personuppgifter i FRA:s uppgiftssamlingar för underrättelser ska bevaras för sådana ändamål.

I FRA-PuL finns dessutom närmare bestämmelser om vem som kan få tillgång till personuppgifter, säkerhetsåtgärder, informationsskyldighet till enskilda samt rättelse och skadestånd m.m.

8.4 Lagen (2000:130) om försvarsunderrättelseverksamhet

Allmänna bestämmelser om försvarsunderrättelseverksamhet finns i lagen (2000:130) om försvarsunderrättelseverksamhet. Lagen anger att sådan verksamhet ska bedrivas till

stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Verksamheten ska bl.a. bedrivas genom teknisk inhämtning, varvid hänvisas vidare till lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (LSF). LSF trädde ikraft den 1 januari 2009 och ändrades i vissa väsentliga delar den 1 december 2009. Vid samma tid infördes också bestämmelser i lagen (2003:389) om elektronisk kommunikation för att skapa en skyldighet för operatörer att överföra trafik till s.k. samverkanspunkter.

I offentlighets- och sekretesslagen (2009:400) finns bestämmelser om sekretess för verksamheten, bl.a. reglerna om försvarssekretess i 15 kap. 2 §. Enligt motsvarande förordning (2009:641) gäller sekretess för uppgifter som rör underrättelseverksamhet inom underrättelse- och säkerhetstjänsten i 70 år.

8.5 Lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

I LSF stadgas att FRA får inhämta signaler i elektronisk form vid signalspaning i sin försvarsunderrättelseverksamhet. Signalspaning får endast ske om regeringen, Regeringskansliet eller Försvarsmakten har gett ett sådant uppdrag till FRA. FRA har alltså inte något eget underrättelseintresse utan är endast den verkställande myndigheten. För att FRA ska få tillräckliga förutsättningar för att kunna bedriva en effektiv försvarsunderrättelseverksamhet får signalspaning också ske i den s.k. utvecklingsverksamheten. Utvecklingsverksamheten syftar till att ge FRA möjlighet att följa förändringar i signalmiljön i omvärlden, följa förändringar i den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, 1 § 3 st LSF. I förarbeten till lagen uttalades att denna verksamhet normalt inte avser innehållet i meddelanden som utväxlas mellan enskilda och att integritetsintrånget därmed blir marginellt. Eftersom verksamheten kan komma att omfatta inhämtning av information om mellan vilka personer viss kommunikation äger rum, kan den ändå vara att anse som känslig ur integritetssynpunkt och bör därför omfattas av de begränsningar som lagen uppställer (prop. 2006/07:63 s.72).

I 1 § LSF finns bestämmelser som anger för vilka syften som signalspaning i FRA:s försvarsunderrättelse- och utvecklingsverksamhet får ske. Signalspaning i tråd får endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör, 2 § LSF. Om signalerna avser kommunikation mellan en avsändare och mottagare som båda befinner sig i Sverige, får kommunikationen dock inte inhämtas, även om signalerna av något skäl förs över Sveriges gräns. Om sådana signaler inte kan avskiljas direkt vid inhämtningen, ska upptagningen eller upptecknigen förstöras så snart det står klart att sådana signaler har inhämtats, 2 a § LSF. Enligt 3 § LSF får signalspaning i tråd endast

ske automatiserat. All automatiserad signalspaning, dvs. även sådan inhämtning som sker i etern, får endast avse signaler som identifierats genom sökbegrepp. Sökbegreppen ska utformas och användas med respekt för enskildas personliga integritet och får endast vara direkt hänförliga till en viss fysisk person om det är av synnerlig vikt för verksamheten, 3 § 2 st LSF.

Signalspaning får endast bedrivas efter tillstånd från Försvarsunderrättelsedomstolen. LSF innehåller närmare bestämmelser om vad en ansökan om sådant tillstånd ska innehålla och under vilka förutsättningar tillstånd får lämnas.

I 7 § LSF finns regler om förstöringsplikt av information som inhämtats. Sådan förstöringsplikt gäller om innehållet berör en viss fysisk person och saknar betydelse för verksamhet enligt 1 § LSF, om inhämtandet strider mot den grundlagsfästa meddelarfriheten i TF och YGL, eller om innehållet avser kommunikation mellan en brottsmisstänkt och dennes försvarare. Förstöringsplikten gäller också om innehållet avser uppgifter som lämnats under bikt och själavård och det inte finns synnerliga skäl att behandla uppgifterna för de syften som LSF anger för signalspaningen.

I lagen hänvisas också till den kontrollmyndighet som utsetts och närmare regleras i förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten (SIUN). SIUN ska särskilt granska sökbegrepp, förstöringsplikt och rapporteringen. Lagen anger också att det inom FRA ska finnas ett särskilt råd som ska utöva fortlöpande insyn för att säkerställa integritetsskyddet i signalspaningsverksamheten.

Om det vid signalspaningen används sökbegrepp som är direkt hänförliga till en viss fysisk person ska denne underrättas om detta enligt 11 a § LSF. Undantag från denna underrättelseskyldighet, bl.a. på grund av sekretess, finns i l lb §.

I LSF regleras vidare SIUN:s uppgift att ge FRA tillgång till signalbärare avseende signaler i tråd. Lagen hänvisar också till reglerna i lagen om elektronisk kommunikation avseende operatörers skyldighet att överföra signaler för att möjliggöra inhämtning samt till reglerna i FRA-PuL om behandling av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten. Enligt förarbeten till LSF (prop. 2008/09:201) täcker LSF och FRA-PuL olika led i processen från inhämtning till rapportering. LSF tar huvudsakligen sikte på inhämtningen, medan FRA-PuL omfattar hanteringen av de uppgifter som har inhämtats och är under fortsatt behandling. Några konflikter mellan de två regelverken föreligger inte enligt regeringens bedömning. I förarbetena uttalas dock att LSF:s bestämmelser, i den utsträckning som de trots allt avser den fortsatta behandlingen, är att anse som specialbestämmelser i förhållande till FRA-PuL. LSF tar därmed över FRA-PuL:s bestämmelser i dessa delar.

9. Vad är signalspaning?

Försvarsunderrättelseverksamheten förser statsledningen och andra uppdragsgivare med information av betydelse för landets utrikes-, säkerhets-, och försvarspolitik. Sveriges förmåga att bedriva underrättelseverksamhet beror till stor del på hur effektiv landets inhämtning med särskilda metoder är eftersom det är dessa uppgifter som sedan ska ligga till grund för bearbetning och analys. Inhämtning med särskilda metoder sker huvudsakligen med hjälp av personbaserad inhämtning och signalspaning. Den personbaserade inhämtningen inom ramen för försvarsunderrättelseverksamheten genomförs av Militära underrättelse- och säkerhetstjänsten (MUST). Den tekniska inhämtningen sker till huvudsaklig del med hjälp av den signalspaning som utförs av FRA. Signaler inhämtas till FRA från kabel, via satellit och genom eterspaning. Signalspaningen syftar till att ge förvarning om förhållanden i omvärlden som kan påverka landet i säkerhetspolitiska och militära hänseenden, t.ex. i form av väpnat angrepp eller kränkningar av Sveriges territoriella integritet. Signalspaningen bedrivs som kommunikationsspaning (KOS) mot utländsk radiokommunikation och som teknisk signalspaning (TES) mot t.ex. radarsignaler. Den utförs från FRA:s inhämtningsstationer, som med hänsyn till radiovågornas utbredning och telenätets egenskaper är placerade på lämpliga platser i Sverige. Spaning bedrivs även från flygplan och fartyg. KOS inriktas mot såväl militära som civila eterburna signaler över kommunikationssatelliter och jordburna system som radiolänkar. Den sändande källans läge bestäms med hjälp av pejling. I allt större utsträckning har signalspaningen utvecklat en förmåga att följa de nya hoten som terrorism och gränsöverskridande organiserad brottslighet.[4] Numera sker signalspaningen även mot signaler som passerar rikets gräns i kabel.

TES inriktas mot signaler med andra syften än kommunikation, främst mot radar- och navigeringssystem. TES används huvudsakligen för att utvinna teknisk information.

De signaler som inhämtas bearbetas, analyseras och sammanställs i rapporter som sänds till FRA:s uppdragsgivare och andra berörda myndigheter. En del av den trafik som FRA inhämtar är krypterad. Bearbetningen inom ramen för kommunikationsspaningen syftar till att forcera signalskyddet och frilägga eller bestämma sändningarnas innehåll. Teknisk analys, trafikbearbetning och kryptoforcering är verktyg för detta. FRA stödjer även Försvarsmaktens internationella verksamhet med signalspaningsutrustning och metodik som behövs för att förvarna om hot mot förbanden, samt med underrättelser under pågående insats.

FRA ska också stödja sådana myndigheter och statligt ägda bolag som hanterar sådan information som är känslig från sårbarhetssynpunkt eller i säkerhetspolitiskt hänseende.

9.1 Hur fungerar inhämtningen av kabeltrafik?

De tekniska förändringarna i samhället och förändrade sätt att kommunicera har inneburit att mycket av den trafik som är intressant för FRA har kommit att förflytta sig från satellit och radio till att bli kabelburen. En konsekvens härav är att det har uppstått ett behov hos FRA att få inhämta signaler som transporteras i kabel. FRA har genom LSF getts möjlighet att under vissa förhållanden spana mot kabeltrafik. Spaningen går till på så sätt att FRA ges tillstånd av Försvarsunderrättelsedomstolen att inhämta signaler i en eller flera signalbärare. Signalbärare är den minsta fysiska beståndsdel i vilka signaler transporteras. Efter det att FRA har fått sitt tillstånd ger Statens inspektion för försvarsunderrättelseverksamheten (SIUN) FRA tillgång till den trafik som finns i de signalbärare som omfattas av domstolens tillstånd. I och med detta har den trafik som finns i de aktuella signalbärarna blivit tillgänglig för FRA. På den trafik som transporteras i signalbärarna applicerar FRA de sökbegrepp som Försvarsunderrättelsedomstolen har godkänt för den aktuella inhämtningen.

9.2 Hur fungerar inhämtningen av satellittrafik?

FRA inhämtar signaler i satelliter genom att utgå från de satellitstråk som är "nåbara" från FRA:s inhämtningsstationer. Inom ramen för utvecklingsverksamheten har FRA skaffat sig kunskap om i vilka stråk som den intressanta trafiken finns. Det är mot dessa stråk som inhämtningen i försvarsunderrättelseverksamhet inriktas. Satellitsignalerna inhämtas med hjälp av antenner och modem och omvandlas därefter till läsbara och hörbara meddelanden som har valts ut med hjälp av sökbegrepp. Inhämtningen av satellittrafik liknar i stora delar inhämtningen i kabel. Även inhämtningen av satellittrafik är tillståndspliktig, men FRA behöver inte ange vilka satellitstråk som inhämtning ska ske i (jfr. signalbärare vid kabelinhämtning). Det finns ca. ett hundratal geostationära satelliter som är nåbara för FRA, men inhämtning kan av resursskäl endast ske samtidigt mot en mindre del av dessa.

9.3 Hur fungerar inhämtning av annan eterbunden trafik?

Inhämtningen av eterburen trafik innebär att signaler, vanligtvis militär trafik, inhämtas med hjälp av antenner som lyssnar av vissa utvalda frekvenser eller sökning efter nya frekvenser med relevant trafik. Exempel på trafik som är eterburen på detta sätt är vissa militära staber, flygplan, fartyg och stridsfordon. Inhämtningen kan ske manuellt, dvs. att en operatör sitter vid inhämtningsutrustningen och i realtid lyssnar på den trafik som förekommer, eller automatiserat genom att inhämtningsutrustningen automatiskt scannar av olika frekvensband och spelar in den trafik som förekommer. När inhämtningen sker automatiserat ska sökbegrepp användas (3 § LSF). Inhämtningen är

tillståndspliktig oavsett om den sker automatiserat eller manuellt. Vid inhämtning av eterburen trafik finns det egentligen inga tekniska parametrar som avgränsar trafiken geografiskt. Dock gäller även här ett förbud mot inhämtning av inhemsk trafik.

10. Personuppgiftsbehandling i samband med FRA:s signalspaning

10.1 Vad är en personuppgift?

Enligt 4 § FRA-PuL avses med begreppet personuppgift *"all slags information som direkt eller indirekt kan hänföras till enskild fysisk person som är i livet".* Som personuppgifter anses således inte bara uppgifter som direkt pekar ut en viss person (såsom namn, personnummer, etc.) utan även andra uppgifter som mer indirekt går att hänföra till en viss enskild person. Exempel på sådana indirekta uppgifter kan vara IP-nummer, telefonnummer, adresser och fastighetsbeteckningar.

I LSF finns bestämmelser om personuppgiftsbehandling, t.ex. i 7 § LSF om förstöringsskyldighet och i 8 § LSF om rapportering. Dessa bestämmelser ska (i enlighet med vad som anförts ovan under 8.5) anses utgöra specialbestämmelser till FRA-PuL. Därutöver finns i 12 § LSF en hänvisning till FRA-PuL vilket innebär att bestämmelserna om personuppgiftsbehandling i FRA-PuL är tillämpliga även inom ramen för den verksamhet som FRA bedriver enligt LSF.

10.2 När behandlar FRA personuppgifter i sin signalspaningsverksamhet?

Datainspektionen har inom ramen för sitt uppdrag strävat efter att få en så heltäckande bild som möjligt av personuppgiftsbehandlingen i FRA:s signalspaningsverksamhet; allt i syfte att kunna identifiera i vilken omfattning som myndigheten behandlar personuppgifter. Inspektionen kan konstatera att inslagen av behandling av personuppgifter vid FRA är mycket omfattande. I princip alla delar av verksamheten inom ramen för såväl utvecklingsverksamheten som försvarsunderrättelseverksamheten innefattar personuppgiftsbehandling i större eller mindre utsträckning. I den trafik som inhämtas av FRA genom signalspaning förekommer vidare i stor utsträckning personuppgifter i form av ljudupptagningar och textmeddelanden. Personuppgifterna förekommer i samtliga skeden av underrättelseprocessen från planläggning, via inhämtning och analys till rapportering. Sammantaget innebär det att förekomsten av integritetsrisker i samband med signalspaning måste undersökas i samtliga delar av FRA:s signalspaningsverksamhet. Att personuppgifter förekommer i så stor omfattning som de gör i signalspaningsverksamheten är dock naturligt. Bakom en stor del av den

signalering som inhämtas av FRA står fysiska personer som kommunicerar med hjälp av telefoner, datorer, faxar och liknande sambandsmedel. De fysiska personerna innehar i sin tur olika befattningar i vilka de kommer i kontakt med och hanterar information som är av betydelse för försvarsunderrättelseverksamheten. För att kunna inhämta den relevanta informationen måste inhämtningen riktas mot de fysiska personernas teleadresser, dvs. telefonnummer, e-postadresser m.m.

10.3 Uppgiftssamlingar vid FRA

En uppgiftssamling är en samling med uppgifter som med hjälp av automatiserad behandling används gemensamt, 4 § FRA-PuL. Enligt 7 § FRA-PuL får FRA, under de förutsättningar som anges i FRA-PuL, behandla personuppgifter i uppgiftssamlingar. I förarbetena till FRAPuL angavs att det att det måste finnas ett stort mått av flexibilitet och förmåga till omvärldsanpassning när det gäller uppgiftssamlingarna (prop. 2006/07:46, sid. 58 ff.). Enligt samma paragraf meddelar således regeringen närmare föreskrifter eller beslut i enskilda fall om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling. 12-6 §§ FRA-PuF har regeringen meddelat föreskrifter om uppgiftssamlingar vid FRA.

Vidare har FRA i interna föreskrifter vid myndigheten meddelat närmare föreskrifter om behandling av personuppgifter i uppgiftssamlingar. Dessa hänvisar till relevanta bestämmelser i FRA-PuL och FRA-PuF. När det gäller själva definitionen av begreppet uppgiftssamling tillämpas inom FRA det synsättet att uppgifter är gemensamt tillgängliga och därför omfattas av bestämmelserna i FRA-PuL och FRA-PuF om uppgiftssamlingar när fler än en (1) person har tillgång till dem. I sak innehåller FRA:s föreskrifter i princip inga egentliga förtydliganden utöver vad som framgår av FRA-PuL och FRA-PuF. När det gäller den behandling som sker ensamt på analytikernas arbetsstationer har Datainspektionen kunnat konstatera att det då främst rör sig om behandling som sker med uppgifter som har extraherats från inhämtningssystemen för vidare bearbetning.

Uppgiftssamlingarna är uppdelade enligt följande.

Råmaterial

Inledningsvis får det enligt 2 § FRA-PuF finnas uppgiftssamlingar för råmaterial. Dessa får endast innehålla obearbetat och automatiskt bearbetat material som har inhämtats i försvarsunderrättelseverksamheten och utvecklingsverksamheten. Information i uppgiftssamlingar för råmaterial ska gallras inom ett år. Av de behandlingar som Datainspektionen har granskat är det endast trafikdata som behandlas i enlighet med 2 § FRA-PuF, dvs. anses utgöra råmaterial, och således gallras efter ett år.

Analysmaterial

Vidare får det vid FRA finnas uppgiftssamlingar för analyser, 3 § FRA-PuF. Dessa uppgiftssamlingar får endast innehålla analysresultat samt bearbetnings- och rapportunderlag. De meddelanden som träffas av sökbegrepp och som samlas i innehållsdatabasen utgör enligt FRA:s synsätt analysmaterial. Information i sådana uppgiftssamlingar ska gallras enligt den allmänna gallringsregeln i 6 kap. 1 § FRA-PuI„ dvs. när uppgifterna inte längre behövs för det ändamål för vilket de behandlas. Denna bestämmelse ger också utrymme för regeringen eller arkivmyndighet att bestämma att uppgifter ska bevaras för historiska ändamål m.m.

Underrättelser

Vid FRA får också finnas uppgiftssamlingar för underrättelser. Det är här endast fråga om färdiga rapporter. Precis som för analysmaterial gäller här i princip den allmänna gallringsregeln i 6 kap 1 §. Krigsarkivet har dock i mars 2009 beslutat att personuppgifter i dessa uppgiftssamlingar får bevaras för historiska, statistiska och vetenskapliga ändamål.

Information om signalmiljön

Uppgiftssamlingar med information om signalmiljön får endast innehålla sådan information och tekniska parametrar som rör signalmiljön. Samlingarna ska gallras vid utgången av det första året efter det att behandlingen påbörjades. Möjligheter till förlängning finns.

Information om företeelser mot vilka signalspaningen inriktas

Slutligen får det vid FRA finnas uppgiftssamlingar för information om företeelser mot vilka signalspaningen inriktas (databasen för spaningsobjekt). Databasen gallras senast vid utgången av det tredje året efter det att behandlingen av uppgifterna påbörjades.

10.4 Behandling av känsliga personuppgifter och behandling av personnummer

Inom ramen för FRA:s signalspaning kan s.k. känsliga personuppgifter komma att inhämtas. Med känsliga personuppgifter avses uppgifter om ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller hälsa, 1 kap. 11 § FRAPuL. De känsliga uppgifterna kan förekomma i meddelanden som dokument (skriftligt) eller i den muntliga kommunikation (foni) som äger rum.

LSF saknar särskilda bestämmelser om behandling av känsliga personuppgifter. Detta regleras däremot i FRA-PuL som enligt 12 a § LSF ska komplettera de bestämmelser som

finns i LSF. Enligt 1 kap. 11 § FRA-PuL får känsliga personuppgifter behandlas av FRA om det är absolut nödvändigt med hänsyn till ändamålet med behandlingen.

Vid FRA finns föreskrifter som rör behandlingen av känsliga personuppgifter.

11. Datainspektionens granskning av FRA:s föreskrifter avseende behandling av personuppgifter

Inom ramen för sitt uppdrag har Datainspektionen lagt ner ett omfattande arbete på att granska de interna föreskrifter som avser personuppgiftsbehandlingen vid FRA. Således har Datainspektionen gått igenom samtliga för personuppgiftsbehandlingen relevanta myndighetsövergripande och avdelningsinterna föreskrifter. Härvid har Datainspektionen inledningsvis kunnat konstatera att en del av föreskrifterna inte helt och hållet har varit uppdaterade utifrån gällande lagstiftning, vilket nu i allt väsentligt har åtgärdats. Dessutom har Datainspektionen genom att spegla de iakttagelser som har gjorts i den praktiska signalspaningsverksamheten kunnat konstatera att vissa bestämmelser inte har varit helt ändamålsenligt utformade för att få avsedd effekt i verksamheten. De frågeställningar som Datainspektionen har haft, har besvarats av FRA vid regelbundna möten. Arbetet med föreskrifterna har således sammanfattningsvis skett på ett sådant sätt att de synpunkter och påpekandet som Datainspektionen har fört fram till stora delar har beaktats av FRA inom ramen för en löpande dialog.

12. Granskningen av ärenden

En viktig del av Datainspektionens arbete har varit att under en längre tid – ca. sex månader –följa personuppgiftsbehandlingen i ett antal utvalda underrättelseärenden vid FRA. Syftet med denna granskning har varit att följa personuppgiftsbehandlingen i försvarsunderrättelseverksamheten samt tillämpningen av lagbestämmelser och interna föreskrifter ur ett praktiskt perspektiv. Härigenom har Datainspektionen, med avstamp i den praktiska signalspaningsverksamheten, kunnat bilda sig en välgrundad uppfattning om vilka konkreta integritetsproblem som kan uppstå. Inspektionen har valt ut tre ärenden med sinsemellan olika inriktning och vid sammanlagt ett tiotal tillfällen per ärende kontrollerat personuppgiftsbehandlingen i dem. Vid granskningstillfällena har ett stort antal meddelanden som sökbegreppen har valt ut för analytikerna för presentation i innehållsdatabasen under denna tidsperiod undersökts på så sätt att de har lyssnats igenom (betr. foni) eller lästs (betr. fax, SMS och e-post). Utöver de meddelanden som väljs ut och som avser innehållet i kommunikationen

använder sig analytikerna i sitt arbete också av uppgifter från databasen för trafikdata. Även denna personuppgiftsbehandling har till viss del granskats.

Datainspektionen har i ärendegranskningen särskilt fokuserat på att undersöka förekomsten av förstöringspliktig information i de meddelanden som har valts ut, samt att i övrigt bilda sig en uppfattning om FRA:s förmåga att kunna välja ut signaler som är relevanta för verksamheten.

13. Informationssäkerhet

Projektgruppens IT-säkerhetsspecialister har genomfört ett antal teknikspecifika och IT-säkerhetsorienterade aktiviteter inom ramen för det aktuella uppdraget. Dessa aktiviteter har utgjorts av möten med teknisk personal och visning av tekniska system, samt en IT-säkerhetsinspektion för att gå igenom administrativa rutiner.

Datainspektionens synpunkter avser sammanfattningsvis följande. Viss genomgång av befintliga verksamhetssystem har redan gjorts för att anpassa dessa till nya regler och arbetsmetoder. Datainspektionen anser dock att ytterligare genomgång kan behöva göras med informationssäkerhet och skydd för den personliga integriteten som utgångspunkt. Dessutom bör hänsyn tas till integritetsfrågor redan i ett tidigt skede vid utveckling av nya system och processer i enlighet med resonemangen om Privacy by Design. Vid behov kan t.ex. befintliga *Bilaga 1* Regeringens (Försvarsdepartementets) uppdrag till Datainspektionen (Fö2009/355/SUND)

Bilaga 1 ***Datainspektionens uppdrag***

Bilaga 2 **Ekonomisk redovisning**