FRA:s signalspaning ur ett rättsligt perspektiv

Av doktoranden Mark Klamberg

I juni 2008 antog riksdagen lagstiftning som innebar en reglering av signalspaning i etern och en rätt för Försvarets radioanstalt att även spana mot kabelkommunikation. Lagförslaget gav upphov till en debatt där lagstiftningens förespråkare betonade behovet av en effektiv försvarsunderrättelseverksamhet och den precision med vilket signalspaning kan bedrivas med vilket enskilda med "rent mjöl i påsen" skulle vara fredade. Kritikerna liknade FRA:s tillgång till den kabelbundna kommunikation vid "massavlyssning", pekade på utvidgningen av FRA:s mandat för signalspaning och oklarheter i avgränsningen mot polisiär verksamhet. Debatten fördes ofta i termer av avlyssning vilket skapat föreställningen att FRA läser och lyssnar på all kommunikation när tekniken och lagstiftningen även medger andra former av övervakning/underrättelseverksamhet. Vidare fanns en fokus på FRA:s försvarsunderrättelseverksamhet där inhämtning av signaler är förhållandevis smal, när myndighetens breda inhämtning av signaler sker inom dess relativt ouppmärksammade utvecklingsverksamhet. Artikeln uppmärksammar särskilt regleringen av dessa två verksamhetsgrenar, FRA:s verktyg för bearbetning av kommunikation och försvarsunderrättelseverksamhetens avgränsning mot polisiär verksamhet.

1. Underrättelseverksamhet och övervakning i den digitala tidsåldern

I samband med riksdagens behandling av Försvarets radioanstalts (FRA) tillgång till kabelbunden kommunikation har det under 2008 förts en intensiv debatt om signalspaning. FRA utför signalspaning med syftet att ge dess uppdragsgivare, däribland regeringen och försvarsmakten, ett informationsöverläge. Under det kalla kriget dominerades hotbilden och därmed FRA:s uppgift av de traditionella säkerhetspolitiska hoten, främst risken för ett storkrig mellan maktblocken i Europa. Motiven till lagförändringar präglas både av förändringar i vår omvärld och ändrade tekniska förutsättningar. Med Berlinmurens fall och östblockets upplösning hösten 1989 har underrättelseinstitutioner som FRA sökt en uppgift. Numera är hotbilden utvidgad till att även omfatta hot som är gränsöverskridande, asymmetriska, icke-militära och som även kan utgå från icke-statliga aktörer. Samtidigt har den teknologiska utvecklingen påverkat formerna för kommunikation där alltmer information förmedlas genom kabel.[1]

[1] Proposition 2006/07:63 "En anpassad underrättelseverksamhet", sid. 16–17, 23; Agrell, Wilhelm, Konsten att gissa rätt — Underättelsevetenskapens grunder, Studentlitteratur, Lund, 1998, sid. 69

Signalspaning är ett av flera verktyg inom underrättelseverksamhet. Underrättelseverksamhet kan även omfatta inhämtning av information genom öppna källor (tidningar, TV- och radiosändningar) och hemliga källor (satellit, spionplan och agenter). Signalspaning kan delas upp i teknisk signalspaning (TES) mot t.ex. radarsignaler och kommunikationssignalspaning (KOS) mot kommunikation i eter och kabel.[2] Denna studie avser FRA:s kommunikationssignalspaning.

En principiell fråga i debatten om signalspaning gäller avvägningen mellan å ena sidan personlig integritet, post- och telehemligheten och å den andra sidan statens intresse av att skaffa tillförlitliga underrättelser. Oenigheten kring lagstiftningens innebörd och avsaknaden av detaljerad information om FRA:s arbetsmetoder har ytterligare komplicerat debatten. Denna studie söker att bemöta dessa utmaningar genom att beskriva FRA:s försvarsunderrättelseverksamhet och utvecklingsverksamhet utifrån dess ändamål, omfattning och metod. Ambitionen är att skapa bättre förutsättningar för en saklig debatt och bedömning om lagstiftningen är i enlighet med Europakonventionens krav.

Underrättelseverksamhet är av naturliga skäl omgärdade av sekretess. Det är olämpligt att offentligt tillgängliggöra material som erhållits från exklusiva källor. Däremot är det naturligt att i en demokrati och rättsstat fortlöpande granska och diskutera underrättelseverksamhetens metoder, målsättningar och prioriteringar.[3]

Ur metodsynpunkt är det en utmaning för FRA att identifiera en begränsad mängd information som är inbäddad i stora kommunikationsflöden. För det fall en terroristcell finns dold bland befolkningen uppstår svårigheter med att finna denna. Det kan liknas vid att finna en nål i en höstack. Frågan i detta sammanhang är hur FRA framgångsrikt ska lyckas med detta när en växande andel av innehållet i meddelanden är krypterat och tendensen är att de blir alltmer svåra att forcera.[4] Det är inte tekniskt möjligt, rättsligt påbjudet eller politiskt önskvärt att FRA söker igenom innehållet i alla meddelanden. Vad är alternativet?

Fakta är att människor i sin kommunikation skapar elektroniska fotspår. Låt oss anta att FRA samlar in all eller stora delar av kommunikationen och granskar vem som är i kontakt med vem. Enbart kryptering av ett meddelandes innehåll erbjuder inget skydd mot sådan övervakning eftersom teleadresserna mellan avsändare och mottagare är kända. Uppgifter om vem som kommunicerar med vem (trafikdata) kan användas för att analysera kommunikationstrafiken varigenom en persons sociala nätverk och ställning i en viss grupp kan kartläggas och fastställas. Vidare är det betydligt lättare att med datorstöd auto-

[2] Prop. 2006/07:63, sid. 22; Agrell, sid. 96
[3] Agrell, sid. 10
[4] SOU 2007:76 Lagring av trafikuppgifter för brottsbekämpning, Betänkande av Trafikuppgiftsutredningen, Stockholm 2007; Agrell, sid. 98 och 122; FRA, publicerad den 14 mars 2007 av Sveriges Television, *Frågor & svar*, fråga 5

matiskt hantera och lagra trafikdata jämfört med att granska innehållet i meddelanden. Ökade möjligheter till trafikbearbetning av kommunikation kan därför ur den enskildes perspektiv vara lika känsligt som om staten tar del av innehållet i enstaka meddelanden. Trafikbearbetning används såväl i polisiär som också militär spaning. I militära sammanhang kan man på detta sätt hitta en ledningsstruktur med högre staber, divisioner, brigader och lägre förband.[5] Det finns ett behov av att diskutera användningen och formerna för denna typ av underrättelseinhämtning.

Denna studie bygger på antagandet att FRA:s signalspaning mot kommunikation kan fungera effektivt om myndigheten inhämtar, lagrar och analyserar stora mängder trafikdata. Därefter kan FRA välja ut den begränsade mängd teleadresser som är relevanta för fortsatt granskning, dvs. forcering av krypto och inhämtning av innehållet i meddelande, vilket vi skulle beskriva som avlyssning. Frågan är om nämnda antagande finner sin motsvarighet i den av riksdagen antagna lagstiftningen.

2. Skydd i Europakonventionen

Inledningsvis kan vi konstatera att kommunikationer mellan enskilda skyddas av både 2 kap. 6 § regeringsformen och artikel 8 i Europakonventionen om de mänskliga rättigheterna. Artikel 8 i Europakonventionen stadgar att var och en har rätt till respekt för sitt privat och familjeliv, sitt hem och sin korrespondens. Europadomstolen har redan prövat två fall som reglerar liknande system som FRA-lagen avser, nämligen Weber och Saravia mot Tyskland och Liberty m.fl. mot Storbritannien.[6] Tillsammans med domstolens tidigare praxis i mål som rört avlyssning, övervakning och registrering ges en bild av vad vilka krav som kan ställas på länder som vill bedriva signalspaning.

Vilken räckvidd har Europakonventionens skydd? Europadomstolen har i sin praxis fastställt att telefonsamtal, fax och e-post omfattas av rekvisiten privatliv och korrespondens.[7] Europadomstolen gör en distinktion mellan att staten tar del av innehållet i ett meddelande och uppgifter om mellan vem kommunikation ägt rum, men även den senare slaget av uppgifter är skyddade av artikel 8.[8] Detta är av be-

[5] Agrell, sid. 97, 120 och 121

[6] Decision as to the Admissibility of Application no. 54934/00 by Gabriele Weber and Cesar Richard Saravia against Germany, ECtHR, 29 juni 2006; Liberty and Others v. the United Kingdom, (Application no. 58243/00), Judgment, 1 juli 2008

[7] Klass and others v. Germany, ECtHR, (Application no. 5029/71), Judgment, 6 september 1978, paras. 41; Malone v. the United Kingdom, (Application no. 8691/79), Judgment, 2 augusti 1984, para. 64; Kruslin v. France, (Application no. 11801/85), Judgment, 24 april 1990, para. 26; Kopp v. Switzerland, (13/1997/797/1000), Judgment, 25 mars 1998, para. 50; Amann v. Switzerland, (Application no. 27798/95), Judgment, 16 februari 2000, para. 44; Weber and Saravia, para. 77; Liberty, para. 56

[8] Malone, para. 84

tydelse då jag påstår och avser visa att FRA samlar in trafikdata i stor omfattning för vidare bearbetning.

Vem omfattas av detta skydd? Europadomstolen har vidare uttalat att en lag som tillåter hemlig övervakning skapar ett hot om övervakning gentemot alla abonnenter som nyttjar tjänsten och därmed ett intrång i det skydd som artikel 8 erbjuder för privatliv, familjeliv och korrespondens.[9]

Under vilka omständigheter är inskränkningar tillåtna? Intrång är tillåtna om dessa har lagstöd, är ägnade att tillgodose vissa legitima ändamål samt är nödvändiga i ett demokratiskt samhälle.[10] Kravet på laglighet omfattar mer än att rättighetsintrånget har stöd i en nationell bestämmelse. Det innefattar även krav på att lagen ska vara förutsebar och tillgänglig.[11] Med kravet på förutsebarhet följer att lagstiftningen ska ha tillräcklig precision för att erbjuda skydd mot godtyckliga intrång.[12] Varje enskild övervakningsåtgärd måste vara förenlig med strikta lagstadgade villkor och tillvägagångssätt.[13] Det finns däremot ingen absolut rätt för den enskilda att bli informerad om att denna blivit avlyssnad eller övervakad.[14] Som en kompensatorisk åtgärd mot denna slutenhet ska det finnas någon form av oberoende kontrollmekanism i form av en domstol eller motsvarande organ.[15]

3. Lagstiftningens grunddrag

Regeringen överlämnade den 8 mars 2007 proposition 2006/06:63 ”En anpassad underrättelseverksamhet” till riksdagen. Efter minoritetsbordläggning antog riksdagen den 18 juni 2008 de delar av regeringens förslag som avsåg signalspaning. Propositionen rörde framförallt en utvidgning av FRA:s mandat för försvarsunderrättelseverksamhet från ”yttre militära hot” till ”yttre hot”.[16] Vidare innehöll den antagna lagstiftningen en ny skyldighet för Internet- och telekomoperatörer att överföra all trafik i kablar som korsar Sveriges gränser till särskilda samverkanspunkter där signaler överlämnas till FRA. Fram till lagändringen har FRA endast kunna inhämta signaler i etern, varvid utgångspunkten varit att skyddet för förtroliga meddelanden inte omfattar exempelvis samtal i folksamlingar eller radiosändningar.

[9] Klass, paras. 37 and 41; Weber and Saravia, para. 78; Liberty, para. 56

[10] Artikel 8(2), Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (ECHR)

[11] Sunday Times v. the United Kingdom, (Application no. 6538/74), Judgment, 26 april 1979, para. 49; Malone, para. 66; Kruslin, para. 27; Kopp, para. 55; Amann, para. 50; Leander v. Sweden, (Application no. 9248/81), Judgment, 26 mars 1987, para. 50; Rotaru v. Romania, (Application no. 28341/95), Judgment, 4 may 2000, para. 52; Foxley v. the United Kingdom, (Application no. 33274/96), Judgment, 20 june 2000, para. 34; Weber and Saravia, para. 84; Liberty, para. 59

[12] Malone, para. 68; Kruslin, para. 33; Kopp, paras. 64 and 72; Amann, para. 56; Weber and Saravia, para. 93

[13] Klass, para. 43

[14] Ibid, para. 58; Weber and Saravia, para. 135; se även Leander, para. 66

[15] Klass, paras. 55–56; Rotaru, para. 59; Weber and Saravia, paras. 117–118

[16] 1 § lag (2000:130) om försvarsunderrättelseverksamhet; Prop. 2006/07:63, sid. 38, 40

FRA:s verksamhet ifråga om signalspaning har därför ej ansett kräva uttryckligt lagstöd utan har bland annat reglerats i den numera upphävda förordningen (1994:714) med instruktion för FRA. Regeringen har dock gjort bedömningen att signalspaning mot kabelburen kommunikation kräver lagstöd eftersom sådan kommunikation är skyddad av både 2 kap. 6 § regeringsformen och artikel 8 i Europakonventionen.[17]

Till saken hör att riksdagen drygt ett år tidigare antagit lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA PuL).[18] Nämnda lagar kompletteras av ett antal förordningar som tillsammans utgör det rättsliga regelverket för FRA:s signalspaning.

I min analys av FRA:s verksamhet kommer jag att följa uppdelningen mellan myndighetens försvarsunderrättelse- respektive utvecklingsverksamhet.[19] Något förenklat kan försvarsunderrättelseverksamheten beskrivas som djup och smal genom att den generar fokuserad underrättelserapportering. Jämförelsevis kan utvecklingsverksamheten beskrivas som ytlig och bred genom att den i sig inte generar underrättelserapportering men samtidigt medför den inhämtning, bearbetning och lagring av en stor mängd uppgifter, även sådana rörande privatpersoners kommunikation som saknar koppling till yttre hot eller dylikt.

Som en följd av den intensiva debatten i frågan har regeringen den 19 december 2008 presenterat en departementspromemoria med förslag om ändringar i den lagstiftning som riksdagen antagit drygt sex månader tidigare, vilket bl.a. medför att endast regeringen, regeringskansliet och Försvarsmakten får inrikta signalspaningen.[20] Denna artikel tar sin utgångspunkt i gällande lagstiftning med endast enstaka hänvisningar till departementspromemorian.

3.1 Försvarsunderrättelseverksamheten

FRA bedriver signalspaning inom ramen för statens försvarsunderrättelseverksamhet, vilket inbegriper inhämtning, bearbetning, analys och rapportering. I förarbetena anges att ”[s]yftet med försvarsunderrättelseverksamheten är att ge stöd för bedömningar och beslut till stöd för svensk utrikes-, säkerhets- och försvarspolitik, att bidra till det svenska deltagandet i internationellt säkerhetssamarbete samt att

[17] Prop. 2006/07:63, sid. 69–70, 88

[18] Proposition 2006/07:46 "Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt"

[19] Utvecklingsverksamhet avser verksamhet för att 1) följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt 2) fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten. Utvecklingsverksamhet används som samlande begrepp endast i lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

[20] Departmentspromemoria Förstärkt integritetsskydd vid signalspaning, 1 § och 4 § första stycket förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

medverka med underrättelser för att stärka samhället vid svåra påfrestningar i fred."[21] Mer precist, får FRA i försvarsunderrättelseverksamheten inhämta signaler i elektronisk form i syfte att kartlägga

1. yttre militära hot mot landet,
2. förhållanden som är relevanta för svenskt deltagande i fredsfrämjande och humanitära internationella insatser samt hot mot svensk personal eller svenska intressen i övrigt under pågående insatser,
3. strategiska förhållanden avseende internationell terrorism eller annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen och krigsmateriel,
5. yttre hot mot samhällets tekniska infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet, och
7. internationella företeelser i övrigt av betydelse för svensk utrikes-, säkerhets- och försvarspolitik.[22]

Ovanstående sju punkter kommer jag fortsättningsvis att benämna som "FRA:s ändamålskatalog".

3.2 Utvecklingsverksamheten

FRA:s utvecklingsverksamhet är en förutsättning för myndighetens signalspaning och omfattar verksamhet för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.[23] I 2 § av den numera upphävda förordningen (1994:714) med instruktion för FRA framgår att myndigheten även tidigare ägnat sig åt denna verksamhet. Det angivna ändamålet med FRA:s utvecklingsverksamhet är att ge tillräckliga förutsättningar för att myndigheten ska kunna bedriva en effektiv försvarsunderrättelseverksamhet, vilket kan verka vagt. I förarbetena ges dock följande exempel på hur utvecklings- och försvarsunderrättelseverksamheten ska samverka med varandra.[24]

> Ett syfte med [utvecklingsverksamheten] är t.ex. att kartlägga vilka kommunikationsvägar som kan vara av intresse för att inhämta information av relevans för försvarsunderrättelseverksamheten.

Denna passage avser den del av utvecklingsverksamheten som syftar att följa förändringar i signalmiljön.[25] Man skulle kunna likna det vid en karta eller telefonbok som FRA använder för att fastställa kommu-

[21] Prop. 2006/07:63, sid. 16
[22] 2 § förordning (2008:923) om signalspaning i försvarsunderrättelseverksamhet
[23] 1 § andra stycket lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet; 1 kap. 9 § FRA PuL.
[24] Prop. 2006/07:46, sid. 68; Prop. 2006/07:63, sid. 72
[25] 1 kap. 9 § punkten 1, FRA PuL; 1 §, andra stycket, punkten 1, lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet

nikationsmönster, sociala nätverk mellan personer och hitta den information som myndigheten vill analysera närmare.

4. Kommunikationssignalspaningens olika steg

För att förstå FRA:s kommunikationssignalspaning behöver vi analysera underrättelseprocessens olika steg närmare: 1) överföring och överlämning, 2) inhämtning, 3) bearbetning (trafikbearbetning inklusive forcering av krypterade meddelanden och innehållsbearbetning) och analys, 4) rapportering och utbyte av information.[26] Därtill kommer lagring av data som kan ske vid olika delar av nämnda faser. Från senare steg, t.ex. analys, sker återkoppling genom att underrättelsebehovet bekräftas eller förändras vilket i sin tur kan leda till att urvalet för inhämtning förändras.[27]

4.1 Överföring och överlämning

I det första steget ska de trådägande operatörerna till särskilda samverkanspunkter överföra all trafik som förs över Sveriges gräns, vilket även kan omfatta kommunikation mellan avsändare och mottagare som befinner sig i Sverige.[28] Lagstiftningen gör här ingen uppdelning mellan försvarsunderrättelse- och utvecklingsverksamhet. Samverkanspunkterna är de platser där trafiken överlämnas från de trådägande operatörerna till FRA. Med hänsyn till hur modern telekommunikation fungerar kan inte svensk trafik sorteras bort i överföringsfasen då valet av kommunikationsväg är automatiserat. Den som använder nätet kan inte bestämma vilken väg eller vilken kombination av medier som skall användas vid ett visst kommunikationstillfälle. Det är inte heller säkert att den geografiskt sett kortaste vägen för överföring används. Kommunikation som till synes sker inom Sverige kan därför ta omvägen via utlandet. Valet sker helt utifrån företagsekonomiska bedömningar med hänsyn till pris och kommunikationskapacitet. Med andra ord, all trafik i de berörda kablarna, oavsett om det rör svensk eller utländsk kommunikation ska överföras till särskilda samverkanspunkter som ytterst kontrolleras av staten.[29] Utifrån Europadomstolens praxis innebär detta ett intrång i privatlivet och korrespondens alldeles oavsett om någon avlyssning sker.[30] Lagrådet har i samma anda anmärkt att intrånget i friheten att kommunicera mellan människor som använder telekommunikationstjänster ”sker

[26] Prop. 2006/07:46, sid. 29

[27] Agrell, sid. 21 beskriver delar av denna process som underrättelsecykeln; National Research Council använder i sin rapport *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, National Academies Press, Washington, DC, 2008, sid. 120–132, uttrycket ”information life cycle” där sju steg används för att beskriva hur digital information behandlas

[28] 6 kap. 19 a § Lag (2003:389) om elektronisk kommunikation; Prop. 2006/07:63, sid. 83; Post- och telestyrelsen, Yttrande den 27 oktober 2005 Departementsskrivelsen om en anpassad försvarsunderrättelseverksamhet (Ds 2005:30), sid. 3–4

[29] Prop. 2006/07:63, sid. 58 och 85

[30] Klass, paras. 37 and 41; Weber and Saravia, para. 78; Liberty, para. 56

redan genom att staten bereder sig tillgång till teletrafiken och inte först när ett visst meddelande avskiljs för analys genom sökbegreppen."[31]

4.2 Inhämtning

Insamling eller inhämtning av information är en nödvändig förutsättning för all underrättelseverksamhet. Genom att operatörerna överför trafiken till samverkanspunkterna blir information tillgänglig för FRA:s inhämtning. Ett avgörande element utöver tillgång till information är selektivitet. Om all information skulle insamlas blir de påföljande leden i processen ogenomförbara.[32] Inhämtningen av signaler är reglerad i 1 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen). Detta lagrum är i sin tur är uppdelad i två stycken, som avser 1) försvarsunderrättelseverksamhet respektive 2) verksamhet för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten. Inhämtning enligt det andra stycket benämner jag med den samlande beteckningen utvecklingsverksamhet. Förståelsen av detta lagrum är central då den reglerar hur mycket information som FRA inhämtar.

4.2.1 Försvarsunderrättelseverksamheten

Den volymmässiga inhämtningen inom ramen för FRA:s försvarsunderrättelseverksamhet är begränsad vilket framgår av 1 § första stycket signalspaningslagen. Den anger följande.

> I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller, enligt regeringens bestämmande, en myndighet närmare bestämt inriktningen av signalspaningen.

Hänvisningen till lagen (2000:130) om försvarsunderrättelseverksamhet är viktig då denna anger försvarsunderrättelseverksamhetens mandat.[33]

> Försvarsunderrättelseverksamhet skall bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Försvarsunderrättelseverksamhet får endast avse utländska förhållanden.

Därmed begränsas inhämtningen av signaler till utländska förhållanden och vissa angivna ändamål som är specificerade i FRA:s ända-

[31] Prop. 2006/07:63, sid. 172
[32] Agrell, sid 28
[33] 1 § första stycket lag (2000:130) om försvarsunderrättelseverksamhet

målskatalog.[34] Det finns ingen begränsning till vilken del av kommunikation som får inhämtas. Nämnda lagrum ger därmed FRA rätt att inhämta innehållet i ett meddelande vilket i ett senare skede gör att ljud i ett samtal eller text i ett meddelande kan avlyssnas respektive läsas.

4.2.2 Utvecklingsverksamheten

Inhämtning kan även ske inom ramen för FRA:s utvecklingsverksamhet. 1 § andra stycket i signalspaningslagen anger att inhämtning av signaler även kan ske utan att det finns krav på någon koppling till FRA:s ändamålskatalog. Med andra ord, FRA får inhämta signaler rörande kommunikation som saknar koppling till yttre militära hot, terrorism eller andra yttre hot. Det aktuella lagrummet anger följande.

> Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att
> 1. följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt
> 2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

Inhämtning inom ramen för FRA:s utvecklingsverksamhet är begränsad till metadata (data om data, såsom t.ex kanalnummer och bärfrekvens). Förarbetena utvecklar saken något och anger att verksamheten ”kan komma att innefatta inhämtning av information, t.ex. om mellan vilka viss kommunikation äger rum, som är känslig ur integritetssynpunkt.”[35] Den tekniska termen för information om mellan vilka viss kommunikation äger rum är trafikdata. Enligt förarbetena ska utvecklingsverksamheten normalt inte avse innehållet i meddelanden.[36]

Här kan nyckeln till förståelse av FRA:s arbetsmetoder finnas. Teleavlyssning enligt 27 kapitlet 18 § rättegångsbalken rör innehållet i meddelanden medan teleövervakning enligt 19 § samma kapitel rör uppgifter om meddelanden, närmare bestämt mellan vilka teleadresser ett meddelande befordrats. Med andra ord, i försvarsunderrättelseverksamheten kan FRA bl.a. ta del av meddelandes innehåll, vilket närmast kan liknas vid teleavlyssning. Genom utvecklingsverksamheten kan FRA inhämta samma slag av uppgifter som är nödvändiga för teleövervakning.

För att underlätta förståelsen ytterligare kan signalspaningslagen jämföras med direktivet (2006/24/EG) om lagring av trafikuppgifter. Direktivet är för närvarande ej genomfört i svensk lag. Direktivet använder termen trafikuppgift vilket motsvarar trafikdata. Av trafikuppgiftsutredningens förslag till förordning om lagring av trafikuppgifter

[34] 2 § förordning (2008:923)
[35] Prop. 2006/07:63, sid. 72
[36] Ibid, sid. 72

m.m. för brottsbekämpande syften framgår att trafikuppgifter bl.a. ska innehålla uppgifter om IP-adress eller telefonnummer för både uppringande part och uppringd part, inklusive uppgift om abonnent och registrerad användare.[37] Jämförelsevis kan konstateras att det finns ingen förpliktelse enligt signalspaningslagen för operatörerna att röja sina abonnenters identitet. Därmed drar jag slutsatsen att FRA avser hantera trafikuppgifter (trafikdata) som anger IP-adress eller telefonnummer, men inte nödvändigtvis abonnentens eller användarens identitet. Med identitet avses namn, fysisk adress och/eller personnummer. Därför har trafikdata en kvalificerad betydelse när vi granskar FRA:s signalspaning.

Som tidigare nämnts överför operatörerna all trafik i de berörda kablarna, vilket kan omfatta avsändare och mottagare av meddelanden som befinner sig i Sverige. Samtidigt finns inget krav på att inhämtning enligt 1 § andra stycket signalspaningslagen ska vara kopplat till yttre hot eller utländska förhållanden. Det innebär att FRA har rätt att inhämta, bearbeta och lagra trafikdata utan att detta nödvändigtvis är kopplad till något hot mot Sverige.[38]

Frågan är i vilken omfattning inhämtning av trafikdata redan har skett inom ramen för eterspaningen och i vilken omfattning det kommer att utökas genom kabelspaningen? Detta anges inte i lagstiftningen eller förarbetena. I samband med att en tjänsteman vid FRA läckt information till SVT Rapport framkom att det handlar om ”generell massinhämtning av trafikdata, där både svenska och utländska medborgares trafikdata samlas in i en bred håv.” Det framkom även att svenskars telefonsamtal och datakontakter samlats in och lagrats i runt tio år i trafikdatabasen Titan. FRA:s generaldirektör Ingvar Åkesson angav att materialet lagrats men att det rensas ut efter 18 månader. Till stöd för dessa uppgifter publicerade SVT ett av FRA:s egna interna dokument från en frågestund med myndighetens medarbetare och ledning. I dokumentet framkommer följande.[39]

1. FRA lagrar redan stora mängder information som därefter söks igenom,
2. FRA skiljer på hanteringen av innehåll och trafikdata,
3. Trafikdata lämpar sig volymmässigt bättre för lagring än innehåll,
4. Trafikdata är ett verktyg för inriktningsbeslut och möjligheten att finna nya urvalsparametrar,
5. FRA anger att de är mycket angelägna om att använda trafikdata även i framtiden,

[37] SOU 2007:76, sid. 40
[38] 1 kap. 4 och 9 §§ FRA PuL
[39] Struwe, Filip, SVT Rapport, *FRA lagrar svenska telesamtal och mejl, 16 juni 2008*; FRA "Frågor & svar", frågorna 5 och 24. Dokumentets autenticitet har bekräftats vid senare tillfällen, bl.a. genom att Justitiekanslern den 27 juni 2008 inledde en förundersökning beträffande läckan. Utredningen lades ner den 3 april 2009 (Dnr 4502-08-31). FRA har själv lämnat ut dokumentet där vissa uppgifter belagts med sekretess, se Aftonbladet, 18 oktober 2008 *FRA fick inte hindra mord — Tidigare hemligstämplade dokument visar hur myndigheten har kunnat tänja på lagen*

6. Med ökad framtida kryptering och ständigt ökande trafikvolymer ökar trafikbearbetningens styrkor i förhållande till den klassiska icke-militära innehållsbearbetningen och
7. De sökbegrepp som styr vad som ska inhämtas kan omfatta ”svenska parametrar”.

Vad innebär detta? Genom lagring och bearbetning av stora mängder trafikdata får FRA ett underlag för beslut om vilken trafik som ska granskas närmare. FRA använder i sitt interna dokument termerna ”trafikbearbetning” och ”innehållsbearbetning”. Samma begrepp återkommer i förarbetena till den antagna lagstiftningen.[40] Det faktum att samma terminologi används i såväl förarbetena som FRA:s interna dokument är viktigt eftersom det skapar en förståelse för relationen mellan lagstiftningen och de metoder som FRA redan och fortsättningsvis avser att använda.

4.2.3 Inhämtning genom sökbegrepp

Av lagen och förarbetena framgår att inhämtningen är automatiserad och signaler identifieras med sökbegrepp vilket möjliggör utsållning av relevant information.[41] FRA beskriver det i sina interna dokument som realtidsfiltrering med applicering av sökbegrepp.[42] Lagrådet är mer utförliga när de beskriver processen som att ”meddelande avskiljs för analys genom sökbegreppen” och att fastställandet av sökbegrepp är av ”synnerlig betydelse för omfattningen av avlyssningen”.[43]

Sökbegrepp ska inte förväxlas med det mer snäva termen ”nyckelord”, t.ex. bomb eller al-Qaida. Om sökbegrepp hade denna snäva betydelse blir slutsatsen lätt att FRA:s datorer söker efter dylika termer i alla meddelanden. Detta är praktiskt svårt av flera skäl, inte minst pga. de stora trafikmängderna och användandet av kryptering. Om utformningen av sökbegrepp även omfattar tekniska parametrar så kan FRA med större effektivitet utnyttja exempelvis trafikdata och trafikbearbetning. I förarbetena förklaras följande.[44]

> För att undvika att irrelevant information inhämtas måste sökbegrepp med hög precision användas. … Utformningen av sökbegrepp för automatiserad inhämtning styrs av ändamålen för verksamheten såsom de angivits i lagen och inriktningen av verksamheten. Den närmare utformningen av sökbegrepp sker bl.a. genom väl avvägda kombinationer av teknisk data (såsom varifrån i världen signalerna inhämtas och med vilka transmissionsmedel de förmedlas) samt andra parametrar som nyckelord (t.ex. det särskilda namnet på ett vapensystem eller annan teknisk terminologi) och unika namn och språk.

[40] Prop. 2006/07:46, sid. 29; Prop. 2006/07:63, sid. 22
[41] 3 § lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet; Prop. 2006/07:63, sid. 92
[42] FRA "Frågor & svar", fråga 15
[43] Prop. 2006/07:63, sid. 172
[44] Ibid, sid. 77

FRA använder alltså sökbegrepp som omfattar allt från personuppgifter som namn och språk till tekniska parametrar. Det senare kan vara frekvenser, e-postadresser och telefonnummer. Olika sökbegrepp används tillsammans i olika konstellationer.[45] Till sin hjälp har FRA en Urvalsdatabas, som innehåller ”information om företeelser mot vilka signalspaningen inriktas”.[46] Närmare rutiner för fastställande och hantering av sökbegreppen ska regleras i FRA:s arbetsordning.[47]

4.3 Innehålls- och trafikbearbetning

FRA använder olika verktyg för att blottlägga meningsfull information i det inhämtade materialet. I bearbetningsstadiet förvandlas inhämtade signaler till underrättelser, dvs. blir värderad och analyserad information som antingen utgör svar på ställda frågor eller underlag för nya frågor som kan återföras till processen.[48] FRA:s fördjupade bearbetning och analys av innehåll sker inom ramen för försvarsunderrättelseverksamheten.[49] Denna verksamhet är begränsad till vissa angivna ändamål och liten i förhållande till den totala mängd kommunikation som överförs till de särskilda samverkanspunkterna. Därför måste FRA ha verktyg för att kunna identifiera den kommunikation som är relevant för innehållsbearbetning. Med innehållsbearbetning avses verksamhet där FRA tar del av innehållet i ett meddelande, som kan vara i form av text eller ljud.

Ett centralt verktyg för att kunna identifiera vilken kommunikation som är relevant för innehållsbearbetning är trafikbearbetning. Förarbetena uttrycker det på följande sätt.[50]

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

Med andra ord, FRA bearbetar trafiken och fastställer vilka trafikmönster som är intressanta. Trafikbearbetningen sker i efterhand genom analys av mönster i trafikdata,[51] dvs. man fastställer vem som kommunicerar med vem. Detta ger myndigheten förmågan att avgöra till eller från vilka telefonadresser och IP-adresser som kommunikationen behöver granskas närmare. Kryptering av innehållet i ett med-

[45] SOU 2003:34 Försvarets underrättelseverksamhet och säkerhetstjänst. Integritet — Effektivitet, sid. 129; Prop. 2006/07:63, sid. 76–77, 90
[46] SOU 2003:34. Försvarets underrättelseverksamhet och säkerhetstjänst. Integritet — Effektivitet, Betänkande av Underrättelsedatautredningen, Stockholm 2003, sid. 17, 129. I författningstexten är Urvalsdatabasen benämnd som ”uppgiftssamlingar för information om företeelser mot vilka signalspaningen inriktas”, 6 § Förordning (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet
[47] Prop. 2006/07:63, sid. 78
[48] Agrell, sid. 28
[49] Prop. 2006/07:46, sid. 67
[50] Ibid, sid. 29
[51] FRA "Frågor & svar", fråga 5

meddelande erbjuder inget skydd mot trafikbearbetning, eftersom det endast förutsätter tillgång till trafikdata.[52] Trafikbearbetning benämns ibland även som trafikanalys.[53]

Förarbetena förklarar inte hur FRA genom trafikbearbetning kan identifiera ”varför” viss kommunikation äger rum. Följande resonemang kan erbjuda en tänkbar förklaring. Om FRA först identifierar vem som kommunicerar med vem och med vilken frekvens (intensitet) denna kommunikation äger rum kan myndigheten även dra andra slutsatser. FRA kan avgöra om dessa personer tillhör en fast grupp eller ett lösare nätverk, vem som är ledare för denna grupp samt om deras kommunikation kan kopplas till aktivitet som är känd genom andra informationskällor. I en amerikansk studie beskriver National Research Council hur brottsbekämpande myndigheter använder metoder (Data Mining) för att identifiera mönster som i regel är kopplad till terrorverksamhet.[54] Liknande metoder för trafikanalys kan i militära sammanhang ge indikationer på att ytterligare förband förts in i ett område, eller att förband försvunnit därifrån.[55] På sådant sätt kan myndigheter som FRA göra mer eller mindre säkra slutsatser om varför en viss kommunikation äger rum. Det finns en viss grad av osäkerhet i slutsatser som endast grundas på trafikbearbetning varför de ska hanteras med försiktighet.

Eftersom utvecklingsverksamheten normalt inte avser innehållet i meddelanden mellan enskilda,[56] måste FRA:s innehållsbearbetning ske inom ramen för försvarsunderrättelseverksamheten. Den senare verksamheten är begränsad, varför volymen meddelanden som läses eller avlyssnas av FRA också blir begränsad. Lagen och förarbetena ger dock ingen information om trafikbearbetningen sker i försvarsunderrättelse- eller i utvecklingsverksamheten. Förmodligen sker det i bägge eftersom trafikbearbetning redan ensamt kan ge underlag för underrättelser. Ytterligare vägledning om sambandet mellan trafikbearbetning och utvecklingsverksamheten får man av följande formulering i förarbetena.[57]

> Ett syfte med [utvecklings]verksamheten är t.ex. att kartlägga vilka kommunikationsvägar som kan vara av intresse för att inhämta information av relevans för försvarsunderrättelseverksamheten.

I nedanstående passage i FRA:s interna dokument om grundforskning diskuteras ett påstående från FRA:s hemsida. Detta avsnitt förtydligar sambandet mellan trafikbearbetning och innehållsbearbetning ytterligare.[58]

[52] SOU 2007:76, sid. 132
[53] Agrell, sid. 97
[54] National Research Council, 2008, sid. 185–217
[55] Agrell, sid. 97
[56] Prop. 2006/07:63, sid. 72
[57] Prop. 2006/07:46, sid. 68
[58] FRA "Frågor & svar", fråga 5

Inom ramen för grundforskningsverksamheten får vi rätt att lagra trafikdata, som bland annat innehåller uppgifter om abonnentnummer eller e-postadress som varit i kontakt med varandra. *Påstående: FRA arbetar på så sätt att all tillgänglig kommunikation lagras. I efterhand görs sökningar i den trafiken* Förfarandet inom grundforskningen att lagra stora mängder information, som sedan söks igenom, liknar väl själva påståendet? *Svar.* Det är helt riktigt att hanteringen av trafikdata skiljer sig från hanteringen av inhämtat innehåll. ... [T]illgången till trafikdata är ett oumbärligt verktyg för såväl inriktningsbeslut som möjligheten att finna nya urvalsparametrar (till exempel om målobjektet bytt till ett annat kontantkort). … Vi är mycket angelägna om att använda trafikdata även i framtiden. Med ökad framtida användning av kryptering och med ständigt ökande trafikvolymer ökar också trafikbearbetningens styrkor i förhållande till den klassiska icke-militära innehållsbearbetningen.

I ovan citerade passage används termen urvalsparameter medan författningstexten använder termen sökbegrepp.[59] Urvalsparametrar är sökbegrepp som används vid inhämtning av signaler.[60] Jag ska nu undersöka sambandet mellan sökbegrepp, trafik- och innehållsbearbetning.

4.3.1 Efterhandssökning i FRA:s databaser

Samtidigt som FRA med hjälp av särskilda sökbegrepp inhämtar signaler så lagrar myndigheten uppgifter i databaser.[61] Sökbegrepp används även för att efter inhämtning söka information i dessa databaser, vilket är relevant vid innehålls- och trafikbearbetning eftersom detta sker i efterhand. Det finns således åtminstone två slag av sökbegrepp, i) sökbegrepp för inhämtning (urvalsparametrar) i realtid och ii) sökbegrepp för efterhandsökning.[62]

I förarbetarna påpekas det att automatiserad behandling av personuppgifter, i synnerhet i samlingar av uppgifter (databaser), ger stora möjligheter att söka och sammanställa information. Dessa möjligheter medför särskilt stora risker för intrång i den personliga integriteten. I syfte att minimera denna risk har det införts förbud mot att behandla personuppgifter ”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” (fortsättningsvis benämnt som känsliga personuppgifter). Det finns dock undantag från denna regel. Om uppgifter behandlas på annan grund får de kompletteras med känsliga personuppgifter. Vid sökning får känsliga personuppgifter användas som sökbegrepp om det är absolut nödvändigt för syftet med behandlingen. Det är således inte nödvändigt att vid användning av en känslig personuppgift som

[59] SOU 2003:34, sid. 131; 3 § lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet
[60] Prop. 2006/07:63, sid. 90
[61] 1 kap. 7§ FRA PuL; 2–6 §§ förordning (2007:261)
[62] FRA "Frågor & svar", fråga 15

sökbegrepp alltid använda ett kompletterande sökbegrepp som inte utgör en känslig personuppgift. Säkerhetspolisen har i sitt remissvar ifrågasatt varför det skall ställas strängare krav i polisens verksamhet än i försvarsunderrättelseverksamheten. Förarbetena betonar att användningen av känsliga uppgifter ska vara absolut nödvändig för syftet med behandlingen,[63] men det är fortfarande oklart varför FRA har lösare tyglar. Det kan bero på att myndighetens underrättelsearbete i första hand riktas mot utländska förhållanden och som regel inte berör svenska medborgare. Därmed blir avgränsningen av mandatet för FRA:s signalspaning avgörande.

4.3.2 Sambandet mellan sökbegrepp, trafik- och innehållsbearbetning

Trafikbearbetningen är ett verktyg för att fastställa vem som kommunicerar med vem, vilket bygger på att FRA samlar in stora mängder trafikdata som därefter söks igenom. Därefter kan FRA fastställa inriktning och särskilda sökbegrepp (omväxlingsvis benämnda som urvals- eller tekniska parametrar) kan användas vid fortsatt inhämtning. Med andra ord, sökbegreppen 1) uppdateras kontinuerligt med stöd av trafikbearbetning, och 2) används för att med hög precision inhämta de meddelanden som ryms inom försvarsunderrättelsens ändamål och inriktning. FRA kan i nästa steg bearbeta och analysera ett meddelandes innehåll, t.ex. i form av text eller ljud. Detta gör att försvarsunderrättelseverksamheten och innehållsbearbetningen endast omfattar en begränsad andel av den samlade trafiken som korsar Sveriges gränser.

Vad får detta för konsekvenser för den enskilde? Det är mycket osannolikt att en laglydig medborgares kommunikation kommer att omfattas av sökbegrepp som kan kopplas till yttre militära hot, terrorism och andra ändamål som anges i 2 § signalspaningsförordningen. Därmed sker ingen inhämtning och analys av innehållet i en sådan persons kommunikation. Däremot sker inhämtning, bearbetning och lagring av signaler i betydligt större omfattning inom utvecklingsverksamheten då den ej är kopplad till de ändamål som anges i 2 § signalspaningsförordningen.

4.3.3 Metoder för trafikbearbetning

Av redogörelsen ovan framgår att FRA lagrar stora mängder trafikdata som lagras och bearbetas. Det framgår inte av lagstiftningen eller förarbetena hur denna trafikbearbetning sker. I en studie utförd av National Research Council (NRC), på uppdrag av USA's Department of Homeland Security, presenteras två metoder för analys och informationsutvinning från stora mängder data (Data Mining) som kan användas var för sig eller i kombination. Dessa kan benämnas som subjektbaserad respektive mönsterbaserad informationsutvinning.[64]

[63] 1 kap. 11 § FRA PuL; Prop. 2006/07:46, sid. 73–75, 124, 132

[64] National Research Council, 2008, sid. 17. Mönsterigenkänning är den etablerade termen som motsvarar mönsterbaserad informationsutvinning, se Ingenjö-

Subjektbaserad informationsutvinning utgår från ett startsubjekt, t.ex. en misstänkt terrorist. Den misstänkte terroristens telefon- och datakontakter identifieras och analyseras vilket ger ett underlag för att bestämma vilka kommunikation som närmare ska granskas. Mönsterbaserad informationsutvinning utgår inte från ett givet startsubjekt utan från mönster, inklusive avvikande kommunikationsmönster, som kan förknippas med ett visst hot, t.ex. terrorism.

För utomstående är det svårt att få insyn i vilken omfattning FRA använder den ena, båda eller en kombination av metoderna. Finns det några svagheter i dessa metoder? Den amerikanska studien diskuterar förekomsten av falska träffar och uppmärksammar rättssäkerhetsproblem om mönsterbaserad informationsutvinning används alltför automatiserat. Studien anger att mönsterbaserad informationsutvinning som baseras på historiska erfarenheter av terroristverksamhet kan vara användbar. Däremot är studien skeptisk till metoder där man endast utgår från avvikande kommunikationsmönster utan att ha en väldefinierad tes om vad som är ett hotfullt mönster eftersom detta skapar en stor mängd falskträffar. Falskträffar kan förbruka redan begränsade utrednings- och analysresurser.[65]

Studien utförd av NRC tar bland annat upp den lagstiftning som omfattar National Security Agency (NSA) och nämnda myndighets arbetsmetoder. NSA är den amerikanska motsvarigheten till FRA. I studien uppmärksammas exempelvis att NSA samlar in uppgifter i ”NSA Call database” om miljontals amerikanska medborgares telefonsamtal,[66] vilket liknar FRA:s insamling av tele- och datakontakter i trafikdatabasen Titan.[67] Lagstiftningen beträffande detta område i USA respektive Sverige är förvisso olika, men det verkar som FRA och NSA har likartade verktyg och arbetsmetoder. Även om det är svårt för utomstående att få insyn i FRA:s arbetsmetoder finns ett intresse av att saken diskuteras eftersom valet av metod kan ha konsekvenser för hur mycket information som ska inhämtas, mängden enskilda som berörs av viss granskning och hur begränsade resurser ska användas. Jag anser att det juridiska regelverket bör formuleras på sådant sätt att informationsutvinningen blir fokuserad, exempelvis genom att uppdragsgivarens behovsbeskrivning måste vara tydlig.

4.4 Rapportering och utbyte av information

4.4.1 Förvarsunderrättelseverksamheten

Från underrättelseorganisationer sker delgivning av det analyserade materialet till dess uppdragsgivare.[68] FRA bedriver försvarsunderrättelseverksamhet på uppdrag av regeringen och dess myndigheter. Av

ren nr 9, 2008, sid. 17. Jag har valt att anpassa texten till den engelskspråkiga begreppsbildningen.

[65] National Research Council, 2008, sid. 78–79

[66] Ibid, sid. 162, 204–25, 218, 229–230, 254–255, 297–298, 300, 314

[67] SVT Rapport, FRA lagrar svenska telesamtal och mejl, 16 juni 2008

[68] Agrell, sid. 29

detta följer att efter inhämtning, bearbetning och analys av information rapporterar FRA underrättelser till berörda myndigheter. Underrättelserna lagras i en särskild uppgiftssamling.[69] Skyldigheten att rapportera underrättelser gäller endast signalspaning som skett inom försvarsunderrättelseverksamheten.[70]

Det internationella underrättelsesamarbetet bygger på ett utbyte av information, varav en del uppgifter kan avse känsliga förhållanden för den enskilde. Underrättelser med personuppgifter får föras över till andra länder eller mellanfolkliga organisationer om det är nödvändigt för att Försvarets radioanstalt skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet.[71] Närmare information om FRA:s utbyte av information med andra länder är svår att finna då den är belagd med sekretess.[72] Viss ledning kan sökas i offentlig information, bl.a. att Sverige och USA undertecknat ett säkerhetsforskningsavtal som möjliggör ett gemensamt forsknings- och informationsutbyte inom det civila säkerhetsområdet, vilket bl.a. omfattar terrorismbekämpning.[73]

4.4.2 Utvecklingsverksamheten

FRA:s utvecklingsverksamhet genererar inte någon underrättelserapportering, men den kompetens som byggs upp hos myndigheten på detta område kommer även andra myndigheter till del genom bistånd i tekniskt avseende.[74] I den del av utvecklingsverksamheten som avser biträde till andra myndigheter får behandlade personuppgifter ej användas för andra ändamål eller lämnas ut i annat fall än då det följer av offentlighetsprincipen.[75] Det framgår av 9 § förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet att andra myndigheters direktåtkomst till FRA:s databaser endast rör underrättelser, vilket indikerar att andra myndigheter ej har direktåtkomst till uppgifter insamlade i utvecklingsverksamheten.

Lagstiftaren försöker till synes bygga upp en mur mellan försvarsunderrättelse- och utvecklingsverksamheten, där den senare omfattar stora mängder kommunikation och inte generar någon underrättelserapportering. Jag ifrågasätter riktigheten i denna bild. Kan FRA i

[69] 2 § lag (2000:130) om försvarsunderrättelseverksamhet; 4 § förordning (2007:261)
[70] Prop. 2006/07:63, sid. 80
[71] 1 kap. 17 § FRA PuL
[72] 2 kap. 1–2 §§ sekretesslagen (1980:100)
[73] Agreement between the Government of the United States of America and the Government of the Kingdom of Sweden on Cooperation in Science and Technology for Homeland Security Matters, 13 april 2007
[74] Prop. 2006/07:63, sid. 72
[75] 1 kap. 10 § FRA PuL; Prop. 2006/07:46, sid. 68. Min tolkning är att ”biträde till andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem” avser samma sak som ”bistånd i tekniskt hänseende” till andra myndigheter (Prop. 2006/07:63 sid. 72). Berörda lagrum och förarbeten lades fram vid olika tillfällen vilket kan förklara skillnaden i terminologi.

förväg veta vilken kommunikation som ska hänföras till respektive verksamhet? Det verkar vara svårt då FRA inledningsvis måste genomföra någon form av analys, t.ex. genom trafikbearbetning. Denna slutsats förstärks av följande passage i förarbetena.[76]

> Eftersom [utvecklingsverksamheten] syftar till att möjliggöra försvarsunderrättelseverksamheten kan det inte anses oförenligt med det ändamål för vilka uppgifterna samlas in att uppgifterna också i viss utsträckning behandlas i försvarsunderrättelseverksamheten.

Det verkar finnas ett kommunicerande kärl mellan de två verksamheterna där uppgifter som ursprungligen samlats in för ett ändamål, t.ex. följa förändringar i signalmiljön, kan användas för ett annat ändamål — i försvarsunderrättelseverksamheten - om FRA finner det påkallat. Jag ser det som ett sammanhängande system snarare än två parallella och isolerade processer.

Frågan är om personuppgifter som inhämtats genom utvecklingsverksamheten får föras över till andra länder och internationella organisationer? Viss ledning ges i 9 § signalspaningslagen som anger att FRA får för utvecklingsverksamheten ”etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.”[77] Innebär detta ett utbyte av data? Om FRA får överföra data som inhämtats genom utvecklingsverksamheten till andra länder så är detta anmärkningsvärt med tanke på att denna verksamhet kan röra stora mängder kommunikation mellan laglydiga individer. Viss trygghet skapas genom att förarbetena anger att det inte är aktuellt med direktåtkomst till FRA:s databaser vid överföring till andra länder.[78] Wilhelm Agrell har förklarat att underrättelsetjänster i allmänhet är obenägna att vidarebefordra rådata — vilket får anses omfattat vad jag benämner som trafikdata — av flera skäl. Utöver behovet av att skydda källor, art och omfattning av utvunnen kunskap så är rådata vanskligt att använda. I fel händer och lösryckt från sitt sammanhang menar Agrell att det kan feltolkas.[79] Samtidigt finns mediauppgifter om det skickas stora mängder rådata från några av baltstaterna till FRA som i sin tur vidareförmedlar data till stora underrättelsenationer som USA.[80] Det är således oklart i vilken omfattning FRA ägnar sig åt utbyte av rådata.

5. Tillstånds- och kontrollfunktion

Tillståndprövning i förhand och efterhandskontroll kommer att utövas av två separata myndigheter, Signalspaningsnämnden respektive Försvarets Underrättelsenämnd (FUN). I syfte att stärka tillstånds-

[76] Prop. 2006/07:46, sid. 68
[77] 9 § lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet
[78] Prop. 2006/07:46, sid. 84
[79] Agrell, sid. 30
[80] NyTeknik, FRA:s metoder granskas efter ny avlyssningsskandal, 27 augusti 2008

funktionen har regeringen lämnat förslag om att Signalspaningsnämnden ska ersättas av en Försvarsunderrättelsedomstol senast den 1 oktober 2009.[81] Enligt den nuvarande lagstiftningen är inriktningen för signalspaning i förvarsunderrättelseverksamhet tillståndspliktig. Detta gäller än så länge bara myndigheter andra än regeringen eller Regeringskansliet, men regeringen har lämnat förslag om att även signalspaning för regeringens behov ska vara tillståndspliktig.[82] Det kan konstateras att utvecklingsverksamheten inte är tillståndspliktig enligt den nuvarande lagstiftningen,[83] men även här har regeringen lämnat lagförslag som medför tillståndsprövning.[84]

Inom ramen för sin kontrollfunktion har FUN en särskild uppgift att kontrollera användningen av sökbegrepp, förstöring av vissa typer av uppgifter och rapportering av underrättelser. FUN ska även granska behandlingen av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten.[85]

6. Gränsdragningen mellan försvarsunderrättelseverksamhet och polisiär verksamhet

Genom att mandatet för försvarsunderrättelseverksamheten även omfattar yttre hot som internationell terrorism och annan gränsöverskridande brottslighet aktualiseras frågan om gränsdragningen mot den verksamhet som bedrivs av polis och andra brottsbekämpande myndigheter. FRA kan enligt regeringens bestämmande lämna andra myndigheter biträde inom ramen för sådan myndighetsutövning som den senare myndigheten har att svara för. Vidare ska myndigheter som ägnar sig åt försvarsunderrättelseverksamhet, i enlighet med regeringens bestämmande, kunna syssla med uppdragsverksamhet för annan myndighets räkning.[86]

SÄPO har i sitt remissvar beskrivit gränsdragningsproblematiken i två dimensioner (civil-/militär säkerhet respektive inre-/yttre säkerhet) som skapar fyra olika kombinationer. SÄPO anger att kombinationen inre/militär säkerhet är utesluten och att kombinationerna

[81] Kommittédirektiv "Inrättande av Signalspaningsnämnden", Dir. 2008:137; Prop. 2006/07:63, sid. 75 och 111; Förordning (2007:852) med instruktion för Försvarets underrättelsenämnd; förslag till lag om Försvarsunderrättelsedomstol i departmentspromemoria Förstärkt integritetsskydd vid signalspaning

[82] 5 § första stycket lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet; jämför samma lagrum i departmentspromemoria Förstärkt integritetsskydd vid signalspaning

[83] 5 § första stycket lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet *e contrario*

[84] 4 a § i förslag till ändring av lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet i Departmentspromemoria Förstärkt integritetsskydd vid signalspaning. Se även sid. 66 i nämnda promemoria: ”På motsvarande sätt ska domstolen bedöma en ansökan som avser signalspaning för att följa förändringar i signalmiljön, den tekniska utvecklingen och signalskyddet samt för att utveckla teknik och metodik med utgångspunkt från vad som i lagen anges om signalspaning för sådana ändamål.”

[85] 10 § första stycket, ibid; 3 § förordning (2007:852)

[86] Prop. 2006/07:63, sid. 40 och 48

inre/civil och yttre/militär säkerhet är okontroversiella. Problemet uppstår framförallt i kombinationen yttre/civil säkerhet där FRA har kompetens och förmåga att samla in information samtidigt som civil säkerhet är en polisiär fråga. Regeringen verkar dela detta synsätt.[87] Därmed uppstår frågan om försvarsunderrättelseverksamhet utgör en parallell verksamhet till SÄPOs verksamhetsgrenar kontraspionage, kontraterrorism och författningsskydd som samtliga kan beröra ”utländska förhållanden”. 4 § första stycket lagen (2000:130) om försvarsunderrättelseverksamhet anger följande.

> Inom försvarsunderrättelseverksamheten får det inte vidtas åtgärder som syftar till att lösa uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet.

Förarbetena förklarar att inom försvarsunderrättelseverksamheten får det inte utövas verksamhet som inrymmer polisiära befogenheter såsom förundersökningsåtgärder enligt rättegångsbalken och tvångsmedelanvändning. Vidare anges att försvarsunderrättelseverksamheten inte heller syftar till att lösa en föreskriven uppgift för brottsbekämpande och brottsförebyggande verksamhet. Däremot anges att även om det inom försvarsunderrättelseverksamheten inte får vidtas polisiära åtgärder så får underrättelseinhämtningen omfatta samma företeelser. Begränsningen i 4 § första stycket av nämnda lag ”träffar endast sådana åtgärder för inhämtning av information som tar sig mer konkreta uttryck än t.ex. inhämtning av signaler i elektronisk form vid signalspaning”.[88] Min tolkning blir därmed att FRA får bedriva signalspaning mot internationell terrorism och annan gränsöverskridande brottslighet så länge som åtgärderna inte är del av en förundersökning.

För det fall signalspaningen använder sökbegrepp som är hänförliga till en viss fysisk person uppstår frågan vad som skiljer denna verksamhet från användande av tvångsmedel som hemlig teleavlyssning och hemlig teleövervakning. En skillnad kan vara att signalspaning mot internationell terrorism och annan gränsöverskridande brottslighet sker i ett tidigare stadium än förundersökning vilket gör att avlyssning eller övervakning kan ske utan att villkoren för hemliga straffprocessuella tvångsmedel är uppfyllda.

Enligt 4 § andra stycket lagen (2000:130) om försvarsunderrättelseverksamhet finns följande undantag från begränsningen i det första stycket.

> Om det inte finns hinder enligt andra bestämmelser, får dock de myndigheter som bedriver försvarsunderrättelseverksamhet lämna stöd till andra myndigheters brottsbekämpande och brottsförebyggande verksamhet.

[87] Säkerhetspolisen remissvar, 11 februari 2005; Prop. 2006/07:63, sid. 40
[88] Ibid, sid. 41, 47–48 och 136

Förarbetena anger att det handlar om biträde med åtgärder som den mottagande myndigheten i och för sig haft rätt att vidta på egen hand, men har otillräckliga resurser för. Som exempel på sådana åtgärder anges biträde med kryptoforcering, tekniskt stöd på informationssäkerhetsområdet och stöd i andra situationer då det är särskilt angeläget att resurserna hos de myndigheter som bedriver försvarsunderrättelseverksamhet kan användas för samhällsviktiga ändamål.[89] Det sistnämnda exemplet förefaller öppna upp den begränsning som lagrummet söker att skapa.

Frågan om försvarsunderrättelseverksamhetens gränsdragning gentemot polisiär verksamhet skapade stor debatt under sommaren 2008. Tidigare försvarsministern Mikael Odenberg som undertecknat lagförslaget skrev på DN Debatt den 23 augusti 2008 följande.

> En viktig poäng med den nya lagstiftningen är tvärtom att den uttryckligen förbjuder försvarsunderrättelseverksamheten att någonsin befatta sig med det som är polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet. Denna tydliga rågång mellan försvarsunderrättelseverksamhet och polisiär verksamhet är helt central ur integritetssynpunkt.

Med hänsyn till hur lagtexten och förarbetena är formulerade ifrågasätter jag om det finns ett sådant uttryckligt förbud och tydlig rågång. Inför hotet att stora delar av lagstiftningen skulle rivas upp av oppositionen och dissidenter från alliansspartierna har regeringen lämnat förslag om lagändringar den 19 december 2008 som bl.a. anger att endast regeringen, regeringskansliet och Försvarsmakten får inrikta signalspaningen. 4 § lagen (2000:130) om försvarsunderrättelseverksamhet lämnas dock oförändrad av förslaget. Detta skulle innebära att myndigheter med brottsbekämpande och brottsförebyggande verksamhet förvisso kan få stöd från FRA, men de kommer inte att ha rätt att inrikta signalspaningen. Detta är resultatet av en politisk kompromiss för att rädda lagstiftningen och FRA:s tillgång till kabelbunden kommunikation. Samtidigt söker regeringen en lösning så att polisen åter ska få tillgång till signalspaningsresurser. Därför har regeringen utsett en särskild utredare, förre SÄPO-chefen Anders Eriksson, för att 1) kartlägga Säkerhetspolisens och Rikskriminalpolisens behov av underrättelseinhämtning avseende utländska förhållanden genom signalspaning, 2) utreda hur detta behov ska kunna tillgodoses på ett rättssäkert och effektivt sätt, och 3) utarbeta författningsförslag.[90] Att skära bort polisens möjligheter att inrikta signalspaningen och samtidigt tillsätta en utredning hur polisen ska kunna få tillgång sådana resurser kan verka schizofrent men sådan är ibland politiken.

[89] Ibid, sid. 136
[90] Kommittédirektiv. Underrättelseinhämtning för vissa polisiära behov. Dir. 2008:120

7. Reflektioner

Vad avser FRA:s stöd till polisen är det viktigt att några saker klarläggs. Om spaningen kommer att använda sökbegrepp som är hänförliga till en viss fysisk person behövs en förklaring vad som skiljer sådana signalspaningsåtgärder från redan befintliga tvångsmedel. Handlar det om tillgång till en större mängd information som automatiskt kan bearbetas, behov av att spana utan brottsmisstanke, intresset av att inte avslöja för operatörerna vem man spanar mot eller något annat? Kan samma resultat uppnås med andra tvångsmedel eller polisiära metoder? Polismetodutredningen (SOU 2009:1) har lämnat förslag om brottsbekämpande myndigheters rätt att i underrättelseverksamhet i hemlighet hämta in uppgifter om viss elektronisk kommunikation. Finns det en överlappning mellan det stöd som FRA kan lämna till brottsbekämpande myndigheter och den underrättelseverksamhet som kan komma att regleras av polismetodutredningens förslag? Hur kan de brottsbekämpande myndigheterna effektivt uppnå sina syften samtidigt som den totala integritetskränkningsnivån hålls nere? Dessa frågor bör diskuteras inom ramen för Anders Erikssons utredning.

För det fall signalspaningsåtgärder till stöd för brottsbekämpande och brottsförebyggande verksamhet kan liknas vid tvångsmedel måste vi försäkra oss om att regelverket har tillräckliga rättssäkerhetsgarantier. Det handlar bl.a. om domstolsprövning när spaningsåtgärder avser en fysisk person. Signalspaning till stöd för brottsbekämpande och brottsförebyggande verksamhet bör endast komma i fråga när den befarade brottsligheten kan antas innefatta vissa särskilt i lag angivna straffbara gärningar. Formuleringen ”grov gränsöverskridande brottslighet” i 2 § förordningen (2008:923) om signalspaning i försvarsunderrättelseverksamhet är vag och exemplifiering i förarbeten framstår som otillräckligt. Detta är viktigt för att skapa förutsebarhet för medborgarna så att den enskilde vet under vilka omständigheter han/hon kan utsättas för signalspaning. Vi bör även diskutera om SÄPO ska få stöd genom signalspaning till alla sina verksamhetsområden eller bara en del av dessa. Jag ifrågasätter om det är lämpligt att signalspaning ska kunna ske till stöd för författningsskyddet då detta framförallt rör extremistmiljöer i Sverige. Ett klarläggande i denna fråga kan verka onödig då FRA endast ska spana efter yttre hot, men kan likväl vara nödvändig för att förebygga eventuella farhågor hos allmänheten om att signalspaningen ska leda till någon form av kontrollsamhälle. Vidare är det viktigt att tydliggöra vilken myndighet som styr spaningen mot yttre hot som internationell terrorism och annan gränsöverskridande brottslighet. För det fall sådan spaning ska bedrivas, finns det skäl för att den operativa verksamheten och spaningsuppdragen ska initieras och i hög grad styras av den beställande myndigheten. Annars finns en risk att spaningen blir planlös och i onödan berör en större mängd enskilda personer samt tar knappa ut-

rednings- och analysresurser i anspråk. Denna ståndpunkt vinner stöd av den redogjorda studien från NRC om olika metoder för informationsutvinning. Innan polisen får tillgång till signalspaningsresurser måste dock frågan ställas om inte befintliga tvångsmedel och polisiära metoder är tillräckliga.

I debatten om FRA:s signalspaning, yttranden från remissinstanser och lagrådet har fokus framförallt varit på avlyssning medan insamlingen av stora mängder trafikdata ej uppmärksammats i samma utsträckning. Mot bakgrund av de krav som artikel 8 i Europakonventionen uppställer för att intrång ska anses vara legitima uppstår åtminstone en fråga. Medan FRA:s avlyssning förefaller vara relativt begränsad är insamlingen av trafikdata betydligt mer omfattande. Uppfyller FRA:s inhämtning och lagring av trafikdata i en bred håv utan närmare urskiljning kraven i artikel 8 om i) förutsebarhet, ii) precision och skydd mot godtyckliga intrång och iii) att varje enskild övervakningsåtgärd måste vara förenlig med strikta lagstadgade villkor och tillvägagångssätt?

Ett synsätt är att trafikdata och andra lagrade uppgifter som inte används i underrättelseproduktion är överskottsinformation. Skyddet för den enskildes integritet fullgörs då genom förstöringsskyldighet och kontroll. Ett problem är att man inte på förhand kan veta vad som är underlag för underrättelseproduktion eller överskottsinformation, vilket gör att även det senare kan komma att granskas. Därmed sker ett intrång såväl vid inhämtning, lagring som bearbetning, oavsett om informationen därefter förstörs. Hur allvarlig är denna del av FRA:s verksamhet ur integritetssynpunkt? Svaret på den frågan beror i hög grad på hur vi betraktar system för elektronisk kommunikation och graderar integritetskränkningar. Den antagna lagstiftningen verkar rangordna lagring av trafikdata och kartläggning av kommunikationsmönster som en lägre integritetskränkning, medan granskning av innehåll är mer allvarligt. Min förhoppning är att Lagrådet vid sin granskning av regeringens förslag om lagändringar uppmärksammar FRA:s utvecklingsverksamhet och hantering av trafikdata i högre grad än tidigare. Därutöver behövs en bredare diskussion om de förändrade förutsättningarna och formerna för övervakning i det digitala samhället.