Signalspaning för polisiära behov

Betänkande
av Utredningen om underrättelseinhämtning för vissa polisiära behov

Stockholm 2009

STATENS OFFENTLIGA UTREDNINGAR
SOU 2009:66

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

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-598 191 91
Ordertel: 08-598 191 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, (SB PM 2003:2, reviderad 2009-05-02)
– En liten broschyr som underlättar arbetet för den som ska svara på remiss.
Broschyren är gratis och kan laddas ner eller beställas på
http://www.regeringen.se/remiss

Textbearbetning och layout har utförts av Regeringskansliet, FA/kommittéservice

Tryckt av Edita Sverige AB
Stockholm 2009

ISBN 978-91-38-23251-4
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Genom beslut den 9 oktober 2008 bemyndigade regeringen chefen för Justitiedepartementet att tillkalla en särskild utredare med uppdrag att, mot bakgrund av förändringar inom försvarsunderrättelseverksamheten, utreda hur Säkerhetspolisens och Rikskriminalpolisens behov av underrättelser om utländska förhållanden ska kunna tillgodoses på ett rättssäkert och effektivt sätt.

Som särskild utredare förordnades samma dag f.d. generaldirektören Anders Eriksson.

Utredaren har i enlighet med direktiven biträtts av en referensgrupp bestående av representanter för riksdagspartierna. Som ledamöter i referensgruppen förordnades fr.o.m. den 24 oktober 2008 Otto von Arnold (kd), Krister Hammarbergh (m), Annie Johansson (c), Margareta Persson (s), Lage Rahm (mp), Cecilia Wigström (fp) och Alice Åström (v).

Sekreterare åt utredningen har varit säkerhetsrådet Johan Sjöö.

Utredningen har antagit namnet Utredningen om underrättelseinhämtning för vissa polisiära behov (Ju 2008:14).

Jag får härmed överlämna betänkandet Signalspaning för polisiära behov (SOU 2009:66).

Mitt uppdrag är med detta slutfört.

Stockholm i juli 2009

Anders Eriksson

/Johan Sjöö

Innehåll

Sammanfattning

Inledning

Av lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet framgår att Försvarets radioanstalt under i lagen angivna förutsättningar får bedriva signalspaning i såväl etern som i tråd. Jag lägger nu fram förslag om att Försvarets radioanstalt ska undantagsvis efter tillstånd av domstol kunna utföra sådan signalspaning även för att tillgodose polisens behov av underrättelser om utländska förhållanden, främst Säkerhetspolisens behov av underrättelser om allvarliga hot mot nationell eller internationell säkerhet, samt att radioanstalten ska få delge polisen information från sådan signalspaning under förutsättning att domstolen gett tillstånd till det. Ett sådant tillstånd ska avse sådan information som är relevant för polisen med beaktande av det ändamål för vilket signalspaningen medgivits av domstolen.

Jag vill redan här framhålla att mitt förslag tagit utgångspunkt i att signalspaning, särskilt spaning i tråd, är en metod som enligt min uppfattning kan leda till omfattande intrång i den personliga integriteten. Jag anser därför att det krävs mycket starka skäl för att tillåta sådan spaning. Min utgångspunkt har därför varit att sådan spaning i tråd som huvudregel inte ska få ske. Om allvarliga hot mot nationell eller internationell säkerhet uppstår kan det dock enligt min mening finnas anledning att göra undantag. Också när det rör sig om så allvarlig brottslighet att gällande rätt medger hemlig teleavlyssning men sådan inte går att anordna kan det enligt min mening undantagsvis finnas skäl att i stället använda signalspaning. Jag anser också att det bör göras inskränkningar i den hittillsvarande friheten att bedriva signalspaning i etern.

I det följande lämnar jag i sammanfattande form en redovisning av mina överväganden och förslag. Den som vill ha en detaljerad bild av förslagens innebörd bör dock läsa hela betänkandet.

Bakgrund

Polisen har använt signalspaning sedan andra världskriget, låt vara att syfte och teknik har skiftat genom åren. Spaningen har bedrivits såväl i egen regi som med stöd av Försvarets radioanstalt. Den signalspaning som har bedrivits har avsett enbart spaning i etern. Någon reglering av verksamheten har inte funnits utan signalspaningen har bedrivits med utgångspunkten att etern har ansetts fri att avlyssna. Under senare år har signalspaningen bedrivits av Försvarets radioanstalt på polisens uppdrag inom ramen för försvarsunderrättelseverksamheten.

Ett lagstiftningsarbete har under ett antal år bedrivits i syfte att förändra försvarsunderrättelseverksamheten. En central förändring har varit att utvidga den signalspaning som Försvarets radioanstalt bedriver inom ramen för försvarsunderrättelseverksamheten till att avse inte bara signalspaning i etern utan också i tråd såvitt avser signaler som förs över Sveriges gräns. En konsekvens av det lagstiftningsarbetet är emellertid att möjligheten för polisen att inom ramen för försvarsunderrättelseverksamheten inrikta signalspaningen vid Försvarets radioanstalt kommer att upphöra.

Mitt utredningsuppdrag har mot denna bakgrund omfattat att kartlägga Säkerhetspolisens och den övriga polisens behov av underrättelser om utrikes förhållanden samt att utreda hur detta behov ska kunna tillgodoses på ett rättssäkert och effektivt sätt.

I uppdraget har också ingått att försöka skaffa information om förhållandena i andra länder när det gäller polisens rätt att få information genom signalspaning. Den information jag inhämtat om detta har visat att det endast i få länder finns mera omfattande lagstiftning härom. I flertalet av de länder som jag undersökt saknas lagstiftning helt eller nästan helt. I samtliga länder som jag undersökt närmare får dock polisen del av information från signalspaning. I åtminstone vissa av dessa länder kan polisen också begära att få signalspaning utförd. I de flesta länderna finns bara en signalspaningsorganisation, som utför signalspaning både åt försvarsunderrättelseverksamheten, säkerhetstjänsten och polisen.

Jag vill i sammanhanget tillägga att det inte varit helt lätt att få information om förhållandena i andra länder. Sekretess och en viss återhållsamhet i uppgiftslämnandet har varit betydande hinder. I vissa fall har återhållsamheten motiverats med hänvisningar till den debatt som förekommit i Sverige kring signalspaningsfrågan.

Det bör tilläggas att lagstiftningsarbetet med avseende på signalspaningen inom försvarsunderrättelseverksamheten ännu inte är avslutat. Ett slutligt ställningstagande i utestående frågor inom ramen för det arbetet kan komma att påverka en del av de förslag som presenteras i detta betänkande.

De förslag som jag lägger fram i detta betänkande gäller bara signalspaning avseende utrikes förhållanden. Signalspaning avseende inrikes förhållanden omfattas alltså inte.

Polisens behov av underrättelser om utrikes förhållanden

Inom såväl den vanliga polisen som inom Säkerhetspolisen finns ett omfattande behov av att kunna få information om utrikes förhållanden. Dagens brottslighet är ofta gränsöverskridande. Brott som riktas mot Sverige eller berör Sverige på annat sätt har ofta sitt ursprung i andra länder. Sverige deltar också i ett internationellt samarbete mot brott. Hot mot nationell eller internationell säkerhet har också ofta internationell anknytning. För att kunna upptäcka, utreda eller förhindra sådan brottslighet eller sådana hot måste den svenska säkerhetstjänsten (Säkerhetspolisen) och den vanliga polisen kunna inhämta underrättelser om utrikes förhållanden. Det kan ske på många olika sätt, t.ex. genom samarbete med andra länders myndigheter och genom egna källor i utlandet. Även signalspaning har under lång tid använts som en inhämtningsmetod.

Signalspaningen ska inte betraktas isolerad, utan måste ses som en metod bland flera andra när det gäller att inhämta information. Genom signalspaning kan polisen t.ex. få sådan information som gör det möjligt att upptäcka brott för att därefter gå vidare med att avstyra den brottsliga verksamheten samt inleda en brottsutredning, eventuellt med användning av tvångsmedel.

När det gäller behovet av att använda signalspaning mot utrikes förhållanden föreligger det stora skillnader mellan Säkerhetspolisen och den övriga polisen. Tyngdpunkten i Säkerhetspolisens arbete är att bedriva s.k. säkerhetsunderrättelsetjänst. I den verksamheten verkar Säkerhetspolisen förebyggande genom att med hjälp av olika metoder undersöka om det t.ex. förekommer säkerhetshotande verksamhet som riktas mot Sverige eller svenska intressen. I den mån sådan verksamhet förekommer är det Säkerhetspolisens uppgift att avstyra verksamheten innan någon skada uppstår. Gemensamt för de typer av säkerhetshotande verksamheter som Säkerhets-

polisen har att motverka – t.ex. spionage, olovlig underrättelseverksamhet och terrorism – är att ursprungen till hoten ofta finns utomlands. Att få kunskap om utrikes förhållanden är därmed nödvändigt för att effektivt kunna motverka den typen av verksamhet. Samtidigt är Säkerhetspolisen en myndighet som saknar befogenhet att agera utanför landets gränser i syfte att inhämta sådan information. Myndigheten måste således få sådan information på annat sätt. Signalspaning genom Försvarets radioanstalts försorg har i det sammanhanget varit en central metod.

Vad gäller den övriga polisen, dvs. Rikskriminalpolisen och polismyndigheterna, är behovet av signalspaning mot utrikes förhållanden mer begränsat. I samband med bekämpning av grov organiserad brottslighet med internationella förgreningar kan emellertid behoven vara liknande de behov som Säkerhetspolisen har. Bekämpning av sådan brottslighet faller i huvudsak under Rikskriminalpolisens ansvar.

Avvägning mot integritetsintresset

Signalspaningens smala tillämpningsområde och inriktningen på utländska förhållanden har säkerligen bidragit till att metoden, såvitt gäller den hittillsvarande spaningen i etern, inte på något tydligt sätt har ifrågasatts från ett integritetsperspektiv. Ett ytterligare skäl torde ha varit att metoden inte har varit känd för en bredare allmänhet.

Vad som nu aktualiserar en tydligare avvägning mellan nyttan av signalspaning och skyddet av enskildas integritet är dels den tekniska utvecklingen med utbyggnaden av det globala nätet, dels frågan om att tillåta signalspaning i tråd. Det globala nätet består av olika kommunikationsvägar som är sammankopplade och som nyttjas gemensamt av teleoperatörer världen över. Utvecklingen går tydligt i riktning mot alltmer av trådbunden trafik.

För signalspaning i etern framstår integritetsintresset som något svagare än för signalspaning i tråd. Att enbart återskapa den möjlighet till signalspaning i etern som polisen använt sig av tidigare framstår emellertid inte som meningsfullt. Betydelsen av signalspaning i etern minskar naturligtvis i takt med att trafiken överflyttas till tråd.

Det går inte att komma ifrån att all signalspaning avseende utrikes förhållanden kan innebära att det görs intrång i enskildas inte-

gritet. Enligt min uppfattning bör därför utgångspunkten vara att polisen inte ska få bedriva sådan signalspaning, varken i etern eller i tråd. I vissa fall kan dock polisens behov av att med hjälp av signalspaning bekämpa viss brottslighet eller vissa säkerhetshot vara så starkt att det vid en avvägning framstår som motiverat att tillåta ett visst intrång i enskildas integritetsskydd. För sådana fall finns det ett behov av att kunna göra undantag från den ovan angivna utgångspunkten. Sådana undantag måste vara noggrant angivna i lag. Vidare måste det införas ett omfattande regelverk till skydd för enskildas personliga integritet. Det måste också kombineras med ett system för insyn och kontroll som motverkar varje form av missbruk.

Mitt förslag innebär därför att polisens hittillsvarande möjlighet att fritt bedriva signalspaning i etern avskaffas och att metoden blir föremål för lagreglering. Det är dessutom med hänsyn till bestämmelserna i Europakonventionen nödvändigt med en sådan lagreglering, om det ska införas möjligheter att undantagsvis signalspana i tråd.

Det bör under inga omständigheter komma i fråga att ge metoden signalspaning en mer generell användning inom polisen. Huvudregeln bör i stället vara att signalspaning inte ska vara tillåten. Varje undantag till en sådan huvudregel bör tydligt framgå av lag och den verksamhet som bedrivs måste vara föremål för insyn och kontroll. Eftersom varje sådant undantag kommer att medföra intrång i den personliga integriteten krävs mycket starka skäl för att tillåta undantag. Inom den vanliga polisens område torde det relativt sällan finnas så allvarliga hot genom brottslig verksamhet att det motiverar att det genom signalspaning görs intrång av detta slag. För den vanliga polisens del måste därför, särskilt när det gäller spaning i tråd, undantagen utformas mycket restriktivt. Annorlunda förhåller det sig vid hot mot nationell eller internationell säkerhet. Här kan hoten ofta vara av så allvarlig karaktär att enskildas intresse av skydd för den personliga integriteten måste få stå tillbaka. Det betyder enligt min mening att utrymmet för att göra undantag från huvudregeln bör vara något större inom säkerhetstjänstens (Säkerhetspolisens) område.

Begränsning av signalspaning i etern

Signalspaning i etern har hittills kunnat användas av polisen utan några begränsningar. Av skäl som angivits ovan begränsas nu polisens rätt att använda sådan spaning avseende utrikes förhållanden till att avse allvarlig brottslighet. Signalspaning i etern bör därför inte få användas för andra brott än sådana för vilka det är föreskrivet fängelse i två år eller däröver.

Som nämnts bör dock säkerhetstjänsten därtill ges möjligheter att använda signalspaning i kampen mot hot mot nationell eller internationell säkerhet. Därför bör Säkerhetspolisen medges rätt att använda signalspaning i etern i syfte att motverka bl.a. olovlig underrättelseverksamhet och andra hot mot rikets säkerhet, utveckling och spridning av massförstörelsevapen, internationell terrorism och annan grov organiserad brottslighet. Gemensamt för dessa områden är att det framstår som särskilt angeläget att Säkerhetspolisen kan skaffa sig kunskap om och följa utvecklingstendenser kring utrikes förhållanden eller där sådan kunskap till och med framstår som avgörande för en framgångsrik verksamhet. Det är vidare områden där ett fullbordat brott allvarligt skulle komma att skada Sverige eller svenska intressen. Det är slutligen områden där Sverige har ett väl etablerat samarbete med andra länder i syfte att öka kunskapen och att motverka brott.

Ytterligare begränsning av signalspaning i tråd

Signalspaning i tråd innebär generellt sett ett något större integritetsintrång än signalspaning i etern. Rätten att bedriva spaning i tråd bör därför kräva ännu starkare skäl än rätten att spana i etern. Användningen av signalspaning i tråd bör begränsas till fall där det framstår som särskilt angeläget med hänsyn till bl.a. rikets säkerhet. Metoden företer, såväl i teknisk mening som med avseende på den kommunikation som är möjlig att inhämta, likheter med hemlig teleavlyssning. En befogenhet att undantagsvis signalspana i tråd bör därför utformas på ett sådant sätt att den strikta regleringen kring hemlig teleavlyssning inte kan kringgås.

Utgångspunkten bör mot denna bakgrund vara att signalspaning i tråd inte får användas av polisen under andra förutsättningar än de som gäller för hemlig teleavlyssning. Det innebär att åtgärden får riktas mot en person som är skäligen misstänkt för brott för vilket

det är förskrivet ett sådant straff som utgör en förutsättning för att använda hemlig teleavlyssning, dvs. ett föreskrivet minimistraff på två års fängelse eller däröver (eller ett straffvärde i det enskilda fallet överstigande två års fängelse). Signalspaning i tråd ska i dessa fall få användas endast då en hemlig teleavlyssning inte är möjlig att genomföra. Som exempel kan nämnas att den misstänkte befinner sig utomlands i ett land där det inte är möjligt att verkställa ett beslut om hemlig teleavlyssning med hjälp av det landets myndigheter.

En utformning av reglerna på nu angivet sätt kommer att innebära att spaning i tråd för den vanliga polisens räkning kommer att få ske endast i enstaka undantagsfall och endast under de förutsättningar som redan gäller för att genomföra en hemlig teleavlyssning.

Därutöver bör Säkerhetspolisen få använda sig av signalspaning i tråd i underrättelsesyfte under i stort samma förutsättningar som föreslås gälla för Säkerhetspolisens signalspaning i etern. Med underrättelsesyfte avses att syftet inte ska vara brottsutredande, dvs. att samla bevis inom ramen för en förundersökning. För att signalspaning i tråd ska få användas mot grov organiserad brottslighet bör dock även krävas att den brottsligheten är av systemhotande karaktär.

Begränsningar i övrigt

Den föreslagna lagstiftningen avser utrikes förhållanden. I syfte att avgränsa tillämpningsområdet bör gälla att signalspaningen inte får avse signaler mellan en sändare och en mottagare som båda befinner sig i Sverige. Avgränsningen gäller för signalspaning i såväl eter som tråd. Om sådana signaler ändå skulle komma att inhämtas ska den informationen omedelbart förstöras.

Vidare bör gälla en proportionalitetsprincip med innebörden att signalspaning endast får ske om syftet med spaningen väger klart tyngre än det integritetsintrång som spaningen kan medföra och vidare en prövning av att det syftet inte kan tillgodoses på ett mindre ingripande sätt. En viktig utgångspunkt vid den bedömningen är att hemlig teleavlyssning bör betraktas som en mindre ingripande åtgärd än signalspaning i tråd. Vidare bör en prövning av proportionaliteten medföra att utrymmet att använda signalspaning för den vanliga polisens räkning, dvs. i huvudsak den typ av eterspaning som hittills

kunnat användas helt fritt, begränsas till brott av mycket allvarlig art, framför allt den gränsöverskridande organiserade brottsligheten.

All signalspaning i tråd ska ske automatiserat och med användning av sökbegrepp. Förutom att en manuell hantering av den oerhört stora mängd trafik som det är fråga om skulle vara betydligt mer resurskrävande, skulle en sådan hantering medföra ökade risker för intrång i den personliga integriteten. Genom kravet på användning av sökbegrepp ökar precisionen i spaningen, vilket får till följd att spaningen inte kommer att ha en bredare inriktning än vad som är absolut nödvändigt för att nå syftet. Automatiserad inhämtning med användning av sökbegrepp kan förekomma också vid signalspaning i etern, men kan i de fallen inte uppställas som ett krav.

Signalspaning i tråd får endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör. Tillgången till de kablar och fibrer som behövs för att genomföra spaningen begränsas till att avse enbart sådana s.k. signalbärare (dvs. fibrer) som är nödvändiga för att utföra uppdraget. På detta sätt begränsas den trafikmängd som signalspaningsmyndigheten får tillgång till för varje enskilt uppdrag avsevärt.

Vem ska utföra signalspaningen?

Signalspaningen bör på polisens begäran utföras av Försvarets radioanstalt, dvs. samma myndighet som har biträtt polisen med signalspaning sedan andra världskriget och som har både det kunnande och den tekniska utrustning som krävs för att genomföra uppdraget.

Alternativet till en sådan lösning, dvs. att låta polisen själv bedriva signalspaning enligt den föreslagna lagstiftningen, skulle vara mycket kostsamt och skulle inte leda till en bättre verksamhet.

För att Försvarets radioanstalt ska utföra signalspaningen för polisens räkning talar också ett annat skäl. Om polisen i Sverige själv skulle få tekniskt genomföra avlyssningen, skulle polisen rent faktiskt komma att besitta mer information än som omfattas av det ändamål för vilket avlyssningen beviljats. Vid inhämtning i tråd skulle visserligen bara den information som befordras i den tillståndsgivna tråden (signalbäraren) komma att inhämtas, men eftersom det i en och samma tråd går inte bara den trafik som polisen fått tillstånd att inhämta utan också annan trafik, skulle en hel del ”överskottsinformation” komma att finnas hos polisen. Även om polisen inte skulle ha rätt att ta del av den sistnämnda, skulle förhållandet att

informationen fanns i polisens hand på goda grunder kunna kritiseras. Genom att föreskriva att polisen inte själv ska få genomföra inhämtningen begränsas polisens tillgång till sådan information som tillståndet att avlyssna avser. Endast denna information ska av Försvarets radioanstalt överföras till polisen. Övrig information stannar hos Försvarets radioanstalt. Härigenom förhindras att polisen får tillgång till en omfattande avlyssning av de internationella kommunikationer som i tråd passerar Sveriges gräns. Polisen får i stället bara tillgång till den information som den ska ha enligt det tillstånd som domstolen givit. Ett motsvarande resonemang kan föras även beträffande avlyssning i etern.

Krav på tillstånd

Signalspaning i såväl etern som i tråd bör förutsätta tillstånd av domstol. Prövningen bör göras av en allmän förvaltningsdomstol, med en möjlighet att överklaga till kammarrätten. Vid prövningen bör, enligt samma modell som gäller vid tillståndsprövning avseende exempelvis hemlig teleavlyssning, medverka ett offentligt ombud med uppgift att bevaka enskildas integritetsintressen.

Ansökan om tillstånd ska göras av polisen, i praktiken Säkerhetspolisen eller Rikskriminalpolisen, med biträde av Försvarets radioanstalt.

Domstolen ska bl.a. pröva om skälen för ansökan om signalspaning är godtagbara utifrån de krav som lagstiftaren ställer. En central uppgift är att pröva ansökan utifrån den föreslagna proportionalitetsprincipen. Domstolen ska därtill bestämma vilka sökbegrepp och vilka signalbärare som ska få användas. Genom en strikt prövning av sökbegrepp och signalbärare begränsas den trafik som signalspaningsmyndigheten får tillgång till samtidigt som precisionen i spaningen ökar. Risken för otillbörliga integritetsintrång minskar därmed avsevärt.

Domstolen får bevilja tillstånd till signalspaning för högst tre månader och får därefter förlänga tiden med högst tre månader i taget.

Det bör finnas möjlighet att i brådskande fall påbörja signalspaning utan domstols tillstånd. En sådan möjlighet bör finnas i de fall syftet med signalspaningen skulle gå förlorat om domstolens tillstånd skulle behöva avvaktas. Om ett sådant beslut skulle fattas – vilket bör ankomma på Försvarets radioanstalt på ansökan av polisen – ska domstolen omedelbart underrättas för att pröva om

signalspaningen ska få fortsätta eller om den omedelbart ska avbrytas.

Förstöring av uppgifter m.m.

Upptagningar eller uppteckningar som gjorts för polisens räkning vid signalspaning ska omedelbart granskas av polisen. De får bevaras endast under vissa angivna förutsättningar och ska därefter förstöras. Uppgifterna får emellertid alltid behandlas enligt de bestämmelser som gäller för polisens verksamhet i övrigt enligt annan lagstiftning.

Vidare bör information som inhämtats genom signalspaning omgående förstöras om innehållet avser uppgifter för vilka tystnadsplikt råder enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen eller som omfattas av förbudet att efterforska meddelare. Detsamma ska gälla för uppgifter som omfattar samtal mellan en misstänkt och dennes försvarare samt som huvudregel om innehållet avser uppgifter lämnade under bikt eller enskild själavård.

Insyn och kontroll

Säkerhets- och integritetsskyddsnämnden bör utöva tillsyn över polisens signalspaning. Nämnden har redan i dag i uppgift att utöva tillsyn över bl.a. polisens användning av hemliga tvångsmedel. Nämnden ska utföra sitt uppdrag genom inspektioner och andra undersökningar.

Nämnden ska vidare på begäran av enskild undersöka om den enskildes kommunikation varit föremål för signalspaning och om spaningen skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen har utförts.

Nämnden bör ha möjlighet att besluta att viss signalspaning ska upphöra eller att upptagning eller uppteckning ska förstöras.

Det finns redan i dag vid Försvarets radioanstalt ett råd för insyn i de åtgärder som myndigheten vidtar för att säkerställa integritetsskyddet i signalspaningsverksamheten. Rådets ledamöter utses av regeringen. Rådet bör ha insyn också i den signalspaning som Försvarets radioanstalt bedriver på uppdrag av polisen.

Författningsförslag

1 Förslag till lag om signalspaning för polisens behov avseende utrikes förhållanden

Härigenom föreskrivs följande.[1]

Inledande bestämmelser

1 § Polisen får använda signalspaning i syfte att avslöja och utreda eller förhindra brott för vilket är föreskrivet fängelse två år eller däröver.

Säkerhetspolisen får använda sådan spaning även i annat fall än som avses i första stycket, om det behövs för att motverka

1. underrättelseverksamhet som kan antas bedrivas av främmande makt eller av organisation som huvudsakligen finns utomlands, om verksamheten är riktad mot Sverige eller svenska intressen eller på annat sätt berör Sverige,
2. annat allvarligt hot mot rikets säkerhet,
3. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
4. internationell terrorism, eller
5. annan grov organiserad brottslighet.

Signalspaning i tråd får ske endast i enlighet med vad som anges i 4–6 §§.

[1] Hänvisningarna till lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, utom såvitt avser hänvisningen i 4 §, avser den föreslagna lydelsen av lagen i prop. 2008/09:201. Förslaget har fogats till detta betänkande som *bilaga 2*.

2 § Signalspaning enligt denna lag får inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen av meddelandets innehåll förstöras så snart det står klart att sådana signaler har inhämtats.

Signalspaningen får ske endast om syftet med spaningen väger klart tyngre än det integritetsintrång som spaningen kan medföra för enskilda och det syftet inte kan tillgodoses på ett mindre ingripande sätt.

3 § Signalspaning ska för polisens räkning utföras av den signalspaningsmyndighet som avses i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Den signalspaningsmyndighet som avses i första stycket får även i övrigt biträda polisen med tekniskt stöd.

Om det är nödvändigt för signalspaning enligt denna lag får signaler i elektronisk form inhämtas även i de syften som anges i 1 § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet. Utan hinder av vad som föreskrivs i 9 § första stycket denna lag ansöker signalspaningsmyndigheten om tillstånd för sådan signalspaning.

Signalspaning i tråd

4 § Inhämtning av signaler i tråd ska ske automatiserat. För sådan inhämtning gäller i övrigt vad som föreskrivs i 2 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

5 § Signalspaning i tråd får ske mot den som är skäligen misstänkt för brott om åtgärden är av synnerlig vikt för utredningen. För brottet får inte vara föreskrivet lindrigare straff än fängelse i två år. Spaningen får dock även avse dels försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff, dels annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Signalspaning i tråd får också ske, om det finns särskild anledning att anta att en person kommer att utöva sådan brottslig verksamhet som avses i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

6 § Signalspaning i tråd får ske för att inhämta underrättelser som avses i 1 § andra stycket 1–4. Om sådan brottslighet som avses i 1 § andra stycket 5 utgör ett hot mot det demokratiska systemet i Sverige eller mot rättssystemet här, får signalspaning i tråd ske för att inhämta underrättelser som behövs för att motverka brottsligheten.

Automatiserad inhämtning

7 § För signalspaning i tråd och annan automatiserad inhämtning gäller i övrigt 3 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Utan hinder av vad som föreskrivs i första stycket får ett sökbegrepp vara direkt hänförligt till en fysisk person, om signalspaningen sker med stöd av 5 § eller om det annars finns särskilda skäl.

Tillstånd

8 § Signalspaning kräver tillstånd. Sådant tillstånd lämnas av Länsrätten i Stockholms län. Tillstånd till signalspaning i tråd ska begränsas till sådana signalbärare som behövs för att uppnå syftet med spaningen. Av domstolens tillstånd ska vidare framgå vilka uppgifter från signalspaningen som får lämnas till polisen.

Tillstånd får ges för högst tre månader. Domstolen får förlänga tiden med högst tre månader i taget.

Vid handläggningen gäller vad som föreskrivs i 27 kap. 26–30 §§ rättegångsbalken.

9 § Ansökan om tillstånd görs av polisen med biträde av signalspaningsmyndigheten. Ansökan ska innehålla uppgift om grunderna för ansökan. Beträffande sådan ansökan gäller i övrigt vad som anges i 4 a § 2–5 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Domstolen får förena ett tillstånd med de villkor som behövs för att begränsa intrånget i enskildas personliga integritet.

Om det för fullgörandet av ett inhämtningsuppdrag för vilket tillstånd redan givits uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp, ska särskilt tillstånd sökas. Ett sådant tillstånd ska ha samma varaktig-

het som tillståndet för det inhämtningsuppdrag inom vilket tillgång till signalerna behövs eller sökbegreppen är avsedda att användas.

10 § Om det kan befaras att inhämtande av domstolens tillstånd skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för något av de i 1, 5 och 6 §§ angivna ändamålen, får tillstånd till signalspaningen ges av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver.

Har tillstånd lämnats enligt första stycket ska åtgärden genast anmälas skriftligen till domstolen. I anmälan ska skälen för åtgärden anges. Domstolen ska då skyndsamt pröva ärendet och, om den finner att det inte finns skäl för åtgärden, upphäva beslutet.

Om ett beslut enligt första stycket har upphört att gälla innan rätten har prövat ett ärende enligt andra stycket, ska åtgärden anmälas till Säkerhets- och integritetsskyddsnämnden.

Tillsyn

11 § Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn över signalspaning som sker enligt denna lag.

Nämnden är skyldig att på begäran av en enskild kontrollera om hans eller hennes kommunikation har inhämtats i samband med signalspaning enligt denna lag eller om uppgifter om den enskilde har inhämtats genom den signalspaningen och lämnats till polisen och bevaras hos polisen eller om polisen i övrigt bevarar sådana uppgifter om den enskilde som inhämtats genom signalspaning. Kontrollen ska särskilt inriktas på om förfarandet skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen har utförts.

För tillsynen gäller i övrigt vad som föreskrivs i 2, 4 och 6 §§ lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Nämnden får besluta att viss inhämtning genom signalspaning ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med lag eller författning eller med tillstånd enligt denna lag eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten.

12 § Vad som föreskrivs i 11 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska tillämpas även för signalspaning enligt denna lag. Vad som där sägs om kontrollmyndigheten ska dock i stället avse Säkerhets- och integritetsskyddsnämnden.

Övriga bestämmelser

13 § Upptagningar, upptecknin gar eller rapporter som gjorts vid signalspaning ska granskas av polisen snarast möjligt. De ska, i de delar de är av betydelse från brottsutredningssynpunkt, bevaras till dess förundersökningen lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar upptagningarna, upptecknin garna eller rapporterna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. De ska därefter förstöras.

Beträffande upptagningar, upptecknin gar eller rapporter som gjorts vid signalspaning gäller i övrigt vad som föreskrivs i 7 § 2–4 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Vad som i 7 § 4 den lagen sägs om syften med behandling av uppgifter ska dock i stället avse de syften som följer av 1, 5 och 6 §§ denna lag.

Trots vad som sägs i första stycket får polisen behandla uppgifter från upptagningar, upptecknin gar och rapporter i enlighet med vad som är särskilt föreskrivet i lag.

14 § Om underrättelser som inhämtats genom signalspaning enligt denna lag kan antas vara av särskild betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, får uppgifterna överlämnas till regeringen, Regeringskansliet eller Försvarsmakten. Om uppgifterna inhämtats inom ramen för en förundersökning får ett sådant överlämnande ske endast om förundersökningsledaren medgivit det.

15 § Vad som föreskrivs i 9 § andra stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska gälla även för verksamhet som signalspaningsmyndigheten bedriver enligt 3 § tredje stycket denna lag.

16 § I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om operatörers skyldighet att överföra signaler för att möjliggöra inhämtning enligt denna lag.

Endast den myndighet som avses i 12 § andra stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska ha rådighet över signalbärare innehållande sådana signaler som överförs i enlighet med de bestämmelser som avses i första stycket. Myndigheten ska ge signalspaningsmyndigheten tillgång till signalbärare endast i den utsträckning som följer av tillstånd enligt 8–10 §§ denna lag.

Denna lag träder i kraft den

2 Förslag till lag om ändring i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

Härigenom föreskrivs i fråga om lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

dels att rubriken ska ha följande lydelse,

dels att 1, 2 och 7 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 8 a §, och närmast före den paragrafen en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Lag om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet	**Lag om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet *m.m.***
	1 §
Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.	Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet *samt i myndighetens verksamhet enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden*, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen (1998:204) gäller inte vid sådan behandling av personuppgifter som anges i första stycket.

2 §

Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

7 §

I Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet får, under de förutsättningar som anges i denna lag, personuppgifter behandlas i uppgiftssamlingar.

Regeringen meddelar närmare föreskrifter eller beslut i enskilda fall om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling.

Personuppgiftslagen (1998:204) gäller inte vid sådan behandling av personuppgifter som anges i första stycket.

2 §

Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet *samt i myndighetens verksamhet enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden.*

7 §

I Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet *samt i myndighetens verksamhet enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden* får, under de förutsättningar som anges i denna lag, personuppgifter behandlas i uppgiftssamlingar.

Regeringen meddelar närmare föreskrifter eller beslut i enskilda fall om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling.

Signalspaning för polisens behov avseende utrikes förhållanden

8 a §

Personuppgifter får behandlas i Försvarets radioanstalts verksamhet enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden om det är nödvändigt för den verksamheten.

Denna lag träder i kraft den

3 Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2003:389) om elektronisk kommunikation att 6 kap. 19 a och 21 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
19 a §	
För att inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet skall kunna ske, är operatörer som äger tråd i vilka signaler förs över Sveriges gräns skyldiga att överföra dessa till samverkanspunkter. Varje sådan operatör skall anmäla en eller flera samverkanspunkter till den myndighet som regeringen bestämmer. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om samverkanspunkter.	För att inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet *och lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden* skall kunna ske, är operatörer som äger tråd i vilka signaler förs över Sveriges gräns skyldiga att överföra dessa till samverkanspunkter. Varje sådan operatör skall anmäla en eller flera samverkanspunkter till den myndighet som regeringen bestämmer. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om samverkanspunkter.
Samtliga operatörer som för signaler i tråd över Sveriges gräns skall till den myndighet som regeringen bestämmer lämna sådan information de innehar som gör det enklare att ta hand om signalerna.	Samtliga operatörer som för signaler i tråd över Sveriges gräns skall till den myndighet som regeringen bestämmer lämna sådan information de innehar som gör det enklare att ta hand om signalerna.
Samtliga operatörer skall utföra uppgifterna enligt första och andra stycket så att verksamheten inte röjs.	Samtliga operatörer skall utföra uppgifterna enligt första och andra stycket så att verksamheten inte röjs.

21 §

Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till

1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,

2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken eller tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål, och

3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till

1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,

2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken eller tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål, och

3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet *och lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden*.

Denna lag träder i kraft den

4 Förslag till förordning om signalspaning för polisens behov avseende utrikes förhållanden

Härigenom föreskrivs följande.

1 § Inom polisen beslutar Rikspolisstyrelsen i frågor om signalspaning för polisens behov.

Beslut att enligt 9 eller 10 §§ lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden begära tillstånd till signalspaning får fattas endast av den som är anställd i ledande befattning hos Rikskriminalpolisen eller Säkerhetspolisen och har tillräcklig juridisk kompetens för uppgiften. Rikspolisstyrelsen ska fortlöpande föra en förteckning över vem som är behörig att fatta sådana beslut.

Har beträffande ett misstänkt brott som signalspaningen ska avse förundersökning inletts och är åklagare förundersökningsledare får ett beslut enligt andra stycket fattas först sedan åklagaren medgett det.

2 § Beslut om ansökan om tillstånd till signalspaning enligt 9 § lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden ska föregås av samråd med den signalspaningsmyndighet som avses i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningsmyndigheten).

3 § Rikspolisstyrelsen ska föra ett register över ansökningar enligt 9 och 10 §§ lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden. Av registret ska framgå om tillstånd till spaning i tråd givits, vilken tid tillståndet avsett, vad spaningen avsett, vilken tid spaningen pågått och vilka uppgifter som erhållits genom signalspaningen. Av registret ska också framgå om upptagningar och uppteckningar som erhållits genom signalspaningen förstörts eller bevarats.

4 § Signalspaningsmyndigheten beslutar efter samråd med Rikspolisstyrelsen om överlämnande av uppgifter enligt 14 § lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden.

5 § Uppgifter som signalspaningsmyndigheten lämnar till polisen med stöd av 2 § lagen (2000:130) om försvarsunderrättelseverksamhet ska lämnas till Säkerhetspolisen eller Rikskriminalpolisen. Har

uppgiften betydelse i förundersökning angående misstanke om brott, får uppgiften även lämnas till den polismyndighet där förundersökningen bedrivs.

6 § Säkerhets- och integritetsskyddsnämnden ska ha tillsyn även över överlämnandet och användningen av sådana uppgifter som avses i 5 §.

Denna förordning träder i kraft den

5 Förslag till förordning om ändring i förordningen (2007:937) med instruktion för Försvarets radioanstalt

Härigenom föreskrivs i fråga om förordningen (2007:937) med instruktion för Försvarets radioanstalt att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Försvarets radioanstalt har till uppgift att bedriva signalspaning i sådan verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet.	Försvarets radioanstalt har till uppgift att bedriva signalspaning *dels* i sådan verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet, *dels enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden*.

Denna förordning träder i kraft den

6 Förslag till förordning om ändring i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden

Härigenom föreskrivs i fråga om förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden att 1 och 9 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Säkerhets- och integritetsskyddsnämnden är en myndighet som ansvarar för de uppgifter som framgår av 1 § lagen (2007:980)om tillsyn över viss brottsbekämpande verksamhet och av 2 och 3 §§ denna förordning.	Säkerhets- och integritetsskyddsnämnden är en myndighet som ansvarar för de uppgifter som framgår av 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet *och av 11 § lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden samt* av 2 och 3 §§ denna förordning.
9 §	
I arbetsordningen får anges att andra ärenden än de som avses i 5 § och 6 § första stycket får avgöras av den som nämnden bestämmer.	I arbetsordningen får anges att andra ärenden än de som avses i 5 § och 6 § första stycket får avgöras av den som nämnden bestämmer.
Utöver vad som följer av första stycket får nämnden, i fråga om tillsyns och kontrollärenden enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet, i arbetsordningen eller genom ett särskilt beslut lämna över till nämndens ordförande eller vice ordförande att fatta beslut av enkel beskaffenhet. Ett sådant överlämnande får dock inte avse behörighet att fatta	Utöver vad som följer av första stycket får nämnden, i fråga om tillsyns och kontrollärenden enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet *och lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden*, i arbetsordningen eller genom ett särskilt beslut lämna över till nämndens ordförande eller vice ordförande att fatta beslut av

beslut om underrättelse till enskild enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet. Beslut som ordföranden eller vice ordföranden har fattat med stöd av ett överlämnande ska anmälas till nämnden på sätt och tid som nämnden bestämmer.	enkel beskaffenhet. Ett sådant överlämnande får dock inte avse behörighet att fatta beslut om underrättelse till enskild enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet *eller 11 § andra stycket lagen om signalspaning för polisens behov avseende utrikes förhållanden*. Beslut som ordföranden eller vice ordföranden har fattat med stöd av ett överlämnande ska anmälas till nämnden på sätt och tid som nämnden bestämmer.
Beträffande de ärenden som avgörs av Registerkontrolldelegationen och Skyddsregistreringsdelegationen finns särskilda bestämmelser om delegering i 24 § tredje stycket och 28 §.	Beträffande de ärenden som avgörs av Registerkontrolldelegationen och Skyddsregistreringsdelegationen finns särskilda bestämmelser om delegering i 24 § tredje stycket och 28 §.

Denna förordning träder i kraft den

1 Uppdraget m.m.

1.1 Uppdraget

Regeringen har i mina direktiv (Dir. 2008:120) som en bakgrund till uppdraget angett att Försvarets radioanstalt endast kommer att bedriva signalspaning i försvarsunderrättelseverksamhet enligt den inriktning som regeringen, Regeringskansliet eller Försvarsmakten bestämmer. Mot den bakgrunden omfattar uppdraget att

- kartlägga Säkerhetspolisens och Rikskriminalpolisens behov av underrättelser om utrikes förhållanden,
- utreda hur detta behov ska kunna tillgodoses på ett rättssäkert och effektivt sätt, och
- lämna fullständiga författningsförslag i frågan.

Av mina direktiv framgår också att jag är fri att ta upp och lämna förslag i näraliggande frågor som aktualiseras under utredningsarbetet.

Direktiven i sin helhet fogas till detta betänkande som *bilaga 1*.

1.2 Utredningsarbetet

1.2.1 Mina utgångspunkter

Detta utredningsuppdrag kan sägas utgöra en del av ett större lagstiftningsarbete som har pågått under flera års tid. De överväganden och förslag som jag redovisar i detta betänkande kan därför inte betraktas isolerade från det lagstiftningsarbete som har pågått relativt länge och som ännu pågår. Det arbetet är i sin tur beroende av redan gjorda ställningstaganden i riksdagen och politiska överenskommelser mellan partierna i regeringen.

För att rätt förstå och bedöma mina överväganden och förslag är det därmed nödvändigt att, i vart fall översiktligt, ta del av det

övriga lagstiftningsarbetet. Följande källor och uttalanden har en avgörande betydelse för vad som har varit möjligt att åstadkomma inom ramen för detta utredningsarbete och kan därmed sägas ha utgjort den yttre ramen för arbetet:

– Inom Försvarsdepartementet utarbetades under åren 2003–2005 promemorian En anpassad försvarsunderrättelseverksamhet (Ds 2005:30). Tre externa utredare förordnades att biträda departementet i arbetet med promemorian. I promemorian förslogs bl.a. en ny lag om signalspaning. Promemorian remitterades.

– Bl.a. mot bakgrund av innehållet i promemorian överlämnande regeringen i mars 2007 till riksdagen propositionen En anpassad försvarsunderrättelseverksamhet (prop. 2006/07:63). Propositionen innehöll bl.a. ett förslag till lag om signalspaning i försvarsunderrättelseverksamhet.

– Riksdagen antog den föreslagna lagen om signalspaning i försvarsunderrättelseverksamhet, men först efter ett års vilandeförklaring. I samband därmed tillkännagav riksdagen att lagen skulle kompletteras med vissa åtgärder i syfte att kringgärda signalspaningen med ytterligare rättssäkerhets- och kontrollmekanismer (se 2007/08:FöU15).

– De partier som ingår i regeringen presenterade därefter under hösten 2008 en överenskommelse med avseende på den av riksdagen antagna lagen. Överenskommelsen innebar att lagen om signalspaning i försvarsunderrättelseverksamhet ytterligare skulle förstärkas med avseende på integritetsskyddet. Överenskommelsen presenterades i punktform och innebar att tillägg och förändringar skulle genomföras, utöver vad riksdagen redan tillkännagivit enligt ovan, på 15 punkter.

– Försvarsdepartementet presenterade kring årsskiftet 2008/2009 promemorian Förstärkt integritetsskydd vid signalspaning (Ds 2009:01). Avsikten var att i promemorian behandla alla de förändringar i lagstiftningen som föranletts av riksdagens tillkännagivande och av vad partierna i regeringen kommit överens om. Promemorian remitterades.

– Regeringen överlämnade den 20 maj 2009 propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) till riksdagen. Förslagen i propositionen är i huvudsak desamma som framgår av den ovan nämnda promemorian. Propositionen har i skrivande stund (juni 2009) ännu inte behandlats av riksdagen.

Mot denna bakgrund har jag i mitt utredningsarbete haft att utgå från den befintliga lagstiftningen om signalspaning i försvarsunderrättelseverksamhet (en lag som alltså såväl riksdagen som regeringen vill reformera och komplettera på ett relativt stort antal punkter), riksdagens tillkännagivande från sommaren 2008, överenskommelsen i punktform mellan partierna i regeringen från hösten 2008, Försvarsdepartementets promemoria från årsskiftet 2008/09 med tillhörande remissynpunkter samt, i ett sent skede av utredningsarbetet, regeringens proposition från maj 2009. En svårighet i sammanhanget har för mig varit att riksdagen ännu inte har klargjort sin syn på hur de överväganden och förslag som presenterats i de olika faserna av lagstiftningsarbetet bör utformas slutligt.

1.2.2 Terminologi m.m.

Lagstiftaren i Sverige har i samband med lagstiftningsarbetet kring signalspaning i försvarsunderrättelseverksamheten valt att använda begreppet signalspaning för att benämna den övervakning och/eller avlyssningsverksamhet som regleras där. Termen signalspaning återfinns även i mina direktiv.

Signalspaning har under flera decennier använts för att beteckna den typ av inhämtning som Försvarets radioanstalt och i viss utsträckning Säkerhetspolisen bedrivit och som avsett spaning mot elektroniska signaler i etern. När det nu är aktuellt för Försvarets radioanstalt att bedriva spaning även med avseende på trådburna kommunikationer blir begreppet signalspaning mindre lätt att avgränsa. Signalspaning, hemlig teleavlyssning och hemlig teleövervakning blir i den meningen olika begrepp för att övervaka och avlyssna samma typ av kommunikationer.

I andra jämförbara länder används andra, mer generella begrepp för att beteckna avlyssning av telekommunikationer, utan avseende på med vilken teknik spaningen genomförs, vem som utför den och vilka syften den har: i Tyskland beskrivet som ”die Telekommunikation zu überwachen und aufzuzeichnen”, i Kanada som ”intercept communications” och i Nederländerna som ”receive and record telecommunications” (officiell översättning till engelska). Benämningarna är teknikneutrala och uttömmande. Termen signalspaning (signal intelligence) används däremot inte i samband med lagstiftning på området och termen har vid mina kontakter med utländska myndigheter snarast skapat viss förvirring.

Det hade enligt min mening varit bättre att mer generellt reglera den övervakning av telekommunikationer som svenska myndigheter har rätt att bedriva samt att i en sådan lagstiftning beskriva för vilka syften sådan övervakning får ske och med vilka begränsningar varje myndighet får bedriva sådan verksamhet. En sådan lagstiftning skulle kunna inkludera både försvarsunderrättelseverksamhetens, säkerhetstjänstens och den vanliga polisens befogenheter på området. Exempel på sådana regelverk beskrivs i samband med redovisningen kring utländska förhållanden (avsnitt 6.2).

Jag har trots allt valt att i mitt förslag använda begreppet signalspaning för att benämna den typ av övervakning av telekommunikationer som bedrivs vid Försvarets radioanstalt, bl.a. på polisens uppdrag. Termen får därmed snarast sin betydelse när det gäller att peka ut vem som ska bedriva övervakningen, inte för att avgränsa vad som är tillåtet eller vilka tekniska metoder som ska tillämpas. Härigenom nås i vart fall en enhetlighet i terminologin med det alltjämt pågående lagstiftningsarbetet avseende signalspaning inom försvarsunderrättelseverksamheten.

Jag har också valt att föreslå en befogenhetslagstiftning för polisen. Den tidigare lösningen – dvs. att polisen tilläts inrikta signalspaningen inom ramen för försvarsunderrättelseverksamheten – har valts bort genom den ovan nämnda politiska överenskommelsen. En befogenhetslagstiftning av den modell jag föreslår motsvarar dessutom den lagstiftning på området som finns i andra jämförbara länder. Inte i något annat land som jag studerat har lagstiftningen utformats som en inriktningslagstiftning. En befogenhetslagstiftning torde dessutom från rättssäkerhetsskäl vara att föredra framför en inriktningslagstiftning.

Jag återkommer nedan till hur förhållandena i Sverige skiljer sig från förhållandena i andra jämförbara länder och vilka konsekvenser dessa skillnader har vad gäller utformningen av mina förslag.

I de utredningsdirektiv som jag fått av regeringen används uttrycket ”Säkerhetspolisens och Rikskriminalpolisens behov av underrättelser om utrikes förhållanden”. Begreppet underrättelse finns inte definierat i lagstiftning. Inte heller i mina utredningsdirektiv eller på annat håll finns någon bestämning av innebörden av detta begrepp. Ordet underrättelse torde få anses vara synonymt med information. Inom polisen torde i vart fall med underrättelse avses detsamma som information. Klart är att underrättelser insamlas inom polisen såväl utan samband med att förundersökning pågår som under förundersökning. Syftet med insamlandet av underrättelser är för polisens del i

första hand att upptäcka, förhindra eller utreda brott (jfr även vad som anförs i avsnitt 7.1.6).

1.2.3 Reflektioner kring den svenska modellen m.m.

Jag redovisar i avsnitt 6 förhållandena i vissa andra länder. En slutsats av den redovisningen är att det är svårt att utan vidare jämföra svenska myndigheter och den svenska lagstiftningen med motsvarigheter utomlands. Svårigheten gör sig gällande såväl vad gäller myndigheternas uppdrag och ansvarsområden som de befogenheter som följer av lag. Sverige har nämligen en organisatorisk struktur som på två punkter avviker från de flesta andra länders.

För det första finns i Sverige finns inte någon civil underrättelsetjänst med uppdrag att inhämta underrättelser om utländska förhållanden, med undantag för den signalspaningsverksamhet som Försvarets radioanstalt bedriver på uppdrag av andra myndigheter inom ramen för försvarsunderrättelseverksamheten.

För det andra är den svenska säkerhetstjänsten, Säkerhetspolisen (SÄPO), en del av polisväsendet och utgör således dels en säkerhetstjänst, dels en polisiär myndighet med ansvar för att utreda brott och som för det ändamålet har polisiära, exekutiva befogenheter. Säkerhetspolisen har inga befogenheter att verka utanför landets gränser och är därmed med avseende på behovet av kunskap om förhållanden utomlands beroende av ett samarbete dels med myndigheterna inom försvarsunderrättelseverksamheten, dels myndigheter i andra länder.

Till denna bakgrund ska läggas att polisen genom den politiska överenskommelsen mellan partierna i regeringen – en överenskommelse som numer också utgör regeringens förslag i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) – inte längre kommer att ha möjlighet att inrikta den signalspaning som bedrivs inom försvarsunderrättelseverksamheten (se avsnitt 4.2). Det saknas därmed möjlighet att i Sverige fortsättningsvis låta sådan spaning bedrivas inom försvarsunderrättelseverksamheten för att därigenom tillgodose polisens behov. Den slutsatsen förstärks av att det av mina direktiv framgår att mina förslag ska utformas på ett sådant sätt att förhållandet mellan signalspaning i försvarsunderrättelseverksamheten och motsvarande underrättelseinhämtning i polisiär verksamhet tydliggörs. Av detta följer att polisens behov av signalspaning måste tillgodoses utan någon koppling till försvarsunderrättelseverksamheten och den signalspaning som bedrivs där.

Inte heller finns möjligheten att låta signalspaningen bedrivas på uppdrag av en civil (dvs. icke-polisiär och icke-militär) myndighet utanför försvarsunderrättelseverksamheten som i sin tur skulle kunna förse svensk polis med underrättelser kring utrikes förhållanden. Någon sådan myndighet med ett självständigt uppdrag att inhämta underrättelser med polisiär relevans, dvs. en motsvarighet de civila underrättelse- och säkerhetstjänster som finns utomlands, finns som nämnts ovan inte i Sverige.

I syfte att uppfylla vad regeringen angett i mina direktiv återstår endast möjligheten att tillgodose den svenska polisens – enligt direktiven både Säkerhetspolisens och Rikskriminalpolisens – behov av signalspaning genom egna befogenheter. En sådan lösning kan självfallet inge betänkligheter av det slag som 11 september-utredningen framförde år 2003:

> Under utredningens arbete har den uppfattningen framförts att möjligheten för FRA att bedriva avlyssning och motsvarande underrättelseinhämtning i kabelbunden trafik bör öka för att denna del av underrättelseverksamheten skall bli mera effektiv inte minst med hänsyn till det ökande hotet mot IT-säkerheten. 11 september-utredningen har förståelse för denna uppfattning, men vill för sin del betona att intresset av säkerhetsunderrättelseverksamhetens effektivitet måste vägas mot vikten av att den personliga integriteten skyddas. Statsmakterna har vid flera tillfällen (se bl.a. prop. 1988/89:124 s. 45 f och 1994/95:227 s. 20) ställt sig avvisande till tanken att telefonavlyssning skall kunna ske i andra fall än när någon är skäligen misstänkt för brott. Spaningsåtgärder för t.ex. polisen som eljest skulle förutsätta domstolsbeslut skall naturligtvis inte kunna fullgöras av FRA genom uppdragsverksamhet.
>
> Utredningen vill emellertid peka på att en ny situation uppstår om i enlighet med vad som förut föreslagits den civila säkerhetstjänsten omvandlas till en från polisen skild myndighet. De betänkligheter, som tidigare bl.a. med tanke på risken för överskottsinformation har gett sig till känna mot en utvidgning eller i varje fall en omreglering av polisens befogenheter på området, har inte samma styrka när det gäller en icke polisiär organisation utan rapporterings- och ingripandeplikt och utan verkställighetsbefogenheter (SOU 2003:32 s. 269 f).

Jag kan instämma i 11 september-utredningens resonemang och slutsatser. Andra lösningar än den jag nu föreslår förutsätter emellertid ändrade politiska ställningstaganden och därtill andra förutsättningar för att utforma förslag än de som framgår av mina direktiv. Den modell som i detta betänkande föreslås för att tillgodose polisens behov av signalspaning kommer därmed också att avvika från modellerna i de länder som redan har reglerat frågan, framför allt såvitt avser befogenheterna för polisiära myndigheter.

Polisen har sedan lång tid tillbaka haft rätt att bedriva signalspaning i etern. I detta betänkande behandlar jag frågan om denna rätt bör begränsas. Jag behandlar också frågan om polisen bör få rätt att signalspana i tråd.

Genom den redan antagna lagen om signalspaning i försvarsunderrättelseverksamhet har Försvarets radioanstalt fått rätt att på uppdrag av vissa särskilt angivna myndigheter bedriva signalspaning i tråd. Sådan spaning medför att Försvarets radioanstalt får tillgång till all den trafik som går i den signalbärare som myndigheten fått tillstånd att signalspana i. Om polisen ska få rätt att låta bedriva signalspaning i tråd kan det enligt min mening inte komma i fråga att polisen på motsvarande sätt skulle få tillgång till all den trafik som går i signalbäraren. I stället måste åtgärder vidtas som gör att polisen bara får tillgång till uppgifter rörande den trafik som rör det fall som omfattas av domstols tillstånd till sådan spaning.

Det är bl.a. mot den nu angivna bakgrunden som jag i det följande föreslår att polisen inte själv ska få bedriva signalspaning, utan att i stället en från polisen fristående myndighet ska genomföra spaningen och därefter för polisen redovisa endast sådant material som omfattas av domstols tillstånd. Det är mot samma bakgrund jag föreslår omfattande bestämmelser kring rättssäkerhet, integritetsskydd samt insyn och kontroll.

Det kan slutligen tilläggas att jag bland de länder som har en liknande myndighetsstruktur som den i Sverige, framför allt de nordiska länderna, inte har funnit någon reglering som motsvarar vad som efterfrågas i mina direktiv.

1.2.4 Samråd

Utredningsarbetet har bedrivits under en relativt kort tid. Jag har samrått med berörda myndigheter, dvs. Säkerhetspolisen, Rikskriminalpolisen, Försvarets radioanstalt och Rikspolisstyrelsen. Jag har även haft fortlöpande kontakter med Regeringskansliet genom Justitiedepartementet och Försvarsdepartementet i syfte att följa det pågående lagstiftningsarbetet där.

Vad gäller de internationella jämförelserna har jag undersökt förhållandena i ett antal länder och har besökt relevanta myndigheter i Kanada, Nederländerna och Tyskland.

Jag har slutligen samrått med Polismetodutredningen (Ju 2008:01).

1.2.5 Referensgruppen

Jag har som stöd för mitt arbete haft tillgång till en referensgrupp med företrädare för riksdagspartierna. Jag har vid sex tillfällen sammanträtt med referensgruppen. Referensgruppen har lämnat synpunkter på utredningens uppdrag och på de överväganden som jag har gjort.

Referensgruppen har bestått av sju ledamöter, en från varje riksdagsparti. Tre ledamöter anser att begränsningarna i direktiven för utredningen omöjliggjort en helhetssyn på hela signalspaningsfrågan. Två av dessa har ansett att endast Säkerhetspolisen och inte den vanliga polisen bör få bedriva eller låta bedriva signalspaning. Den tredje ledamoten har invänt mot att svenska myndigheter över huvud taget ska få använda signalspaning. Denne ledamot har emellertid samtidigt förklarat att om statsmakterna ändå anser att det ska finnas möjlighet för polisen att bedriva eller låta bedriva signalspaning, så är förslaget i och för sig i stort rimligt avvägt. Även denne ledamot anser emellertid att endast Säkerhetspolisen och inte den vanliga polisen bör ha tillgång till signalspaning.

Övriga fyra ledamöter i referensgruppen har hänvisat till det uppdrag som ges i utredningens direktiv vad gäller Säkerhetspolisens och Rikskriminalpolisens behov av underrättelser och har därmed ställt sig tveksamma till om polisen bör få använda signalspaning i brottsutredande syfte. Jag har när det gäller signalspaning i tråd kommit till i huvudsak samma ståndpunkt som dessa fyra ledamöter av referensgruppen. Mitt förslag innebär således att den omständigheten att polisen bedriver en förundersökning om brott inte ska få utgöra grund för att signalspaning i tråd ska få ske. Jag anser dock, som kommer att framgå i det följande, att det behövs ett mindre undantag från denna huvudregel. Om de redan i gällande rätt uppställda förutsättningarna för hemlig teleavlyssning i och för sig är uppfyllda men sådan avlyssning i praktiken inte kan anordnas, anser jag att signalspaning i tråd ska kunna ske, om domstolen ger tillstånd till det (se avsnitt 7.5 om de närmare förutsättningarna för detta undantagsfall). I sammanhanget kan det vara värt att nämna att det i andra länder, t.ex. Tyskland, Kanada och Nederländerna (se avsnitt 1.2.2) inte görs någon skillnad i lagstiftningen mellan hemlig teleavlyssning och signalspaning. Lagstiftningen i dessa länder talar bara om avlyssning eller övervakning av telekommunikation, varmed avses både det som vi i Sverige benämner signalspaning och det som vi här kallar hemlig teleavlyssning. Att

som jag vill skapa likartade regler för hemlig teleavlyssning och signalspaning i tråd i enskilda fall är således i linje med ett sådant synsätt. Som framgår av vad som anförts under avsnitt 1.1 ovan ryms ett sådant förslag också inom ramen för mina utredningsdirektiv (jfr. även vad som anförts under avsnitt 1.2.2).

I övrigt har ledamöterna i referensgruppen förklarat sig nöjda med förslagen i stort.

Beträffande detaljerna i förslagen har det i flertalet fall inom referensgruppen inte funnits några avvikande uppfattningar. I den mån sådana uppfattningar har förekommit redovisas detta under de avsnitt som behandlar de olika sakfrågorna.

2 Allmänt om signalspaning

2.1 Vad är signalspaning?

Signalspaning bedrivs genom inhämtning av signaler i elektronisk form. Den kommunikation som spaningen riktas mot kan förmedlas via olika tekniker såsom Internet, radio eller telenät. Signalerna kan därtill vidarebefordras via olika medium såsom kablar, länkar eller radiovågor.

Trådlös överföring sker på marken genom radiolänkar samt över längre avstånd via kortvåg eller kommunikationssatelliter. Trådburen överföring sker via kablar, t.ex. fiberoptiska nät.

Ett elektroniskt meddelande kan naturligtvis riktas direkt från en avsändare till en mottagare, t.ex. trådburet via ett slutet kabelnät. Det mesta av dagens kommunikation förmedlas emellertid i det s.k. globala nätet. De olika kommunikationsvägarna i det globala nätet är i huvudsak civila och sammankopplade och nyttjade gemensamt. Valet av väg och medium (radiolänk, satellit eller tråd/kabel) styrs av operatörerna, dvs. statliga eller privata kommunikationsföretag. Valet av kommunikationsväg inom det globala nätet är i princip automatiskt, dvs. användaren av kommunikationstjänsterna kan inte välja vilken väg eller vilken kombination av medier som ska användas för ett enskilt meddelande. Det är inte heller så att den geografiskt kortaste vägen att förmedla ett meddelande alltid används. Ett och samma meddelande i det globala nätet kan därmed komma att förmedlas såväl i tråd som i luften.

Signalspaning kan, såvitt här är av intresse, bedrivas i form av fjärrspaning och närspaning. Med fjärrspaning avses avlyssning av signaler där avsändaren finns utanför Sveriges gränser och som riktas mot en mottagare i Sverige eller utomlands, medan närspaning innebär avlyssning av signaler där avsändaren och mottagaren finns i Sverige.

2.2 Den rättsliga grunden för signalspaning

2.2.1 Principen att etern är fri

Av 2 kap. 6 § regeringsformen följer att varje medborgare i Sverige är gentemot det allmänna skyddad mot bl.a. kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Om inte annat är särskilt föreskrivet i lag är utlänningar som befinner sig i Sverige i detta avseende likställda med svenska medborgare (2 kap. 22 § andra stycket 3 regeringsformen).

Skyddet i 2 kap. 6 § regeringsformen är relativt i den meningen att det under vissa förutsättningar får begränsas genom lag. En sådan begränsning får göras endast för att tillgodose ändamål som är godtagbart i ett demokratiskt samhälle. Begränsningen får heller inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Slutligen får en sådan begränsning inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 12 § regeringsformen).

En utgångspunkt som historiskt synes ha haft allmän acceptans är att etern är fri att avlyssna, dvs. det har inte för polisens del krävt något uttryckligt lagstöd att bedriva signalspaning mot luftburen kommunikation. Signalspaning mot eterburen trafik har därmed varit en oreglerad verksamhet, dvs. någon lagstiftning med stöd av 2 kap. 12 § regeringsformen har inte ansetts nödvändig.

Uppfattningen synes ha sin främsta grund i ett förarbetsuttalande. Av förarbetena till bestämmelsen i 2 kap. 6 § regeringsformen följer att skyddet för förtroliga meddelanden inte omfattar exempelvis samtal i folksamlingar eller radiosändningar (prop. 1975/76:209).

Resonemanget får därtill stöd av bestämmelsen i 6 kap. 17 § andra stycket lagen (2003:389) om elektronisk kommunikation av vilken framgår att det inte finns något förbud mot att utan samtycke i en radiomottagare avlyssna ett radiobefordrat elektroniskt meddelande som inte är avsett för den som avlyssnar eller för allmänheten. Av 6 kap. 20 § samma lag framgår att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till vissa uppgifter om bl.a. innehållet i ett elektroniskt meddelande inte

obehörigen får föra vidare eller utnyttja det han fått del av eller tillgång till. Tystnadsplikten gäller inte i förhållande till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller på annat sätt har sänt eller tagit emot meddelandet. I förarbetena anförs att i bestämmelsen i 6 kap. 17 § klargörs den gällande principen om att etern är fri och att var och en i princip fritt kan lyssna till radiobefordrade meddelanden i en radiomottagare. Det konstateras emellertid att reglerna om tystnadsplikt kan vara tillämpliga (prop. 2002/03:110 s. 396).

Principen att etern är fri har numer ifrågasatts. Lagrådet har i yttrande den 9 februari 2007 över förslaget till lagen om signalspaning i försvarsunderrättelseverksamhet anfört att principen allt mer torde kunna ifrågasättas när en allt större del av vår privata kommunikation blir eterburen. Lagrådet framhåller att bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning inte gör någon skillnad mellan fast telefoni och mobil trådlös telefoni och att Europadomstolen i sin praxis har ställt samma krav på villkoren för avlyssning av trådlös kommunikation som i fråga om annan telekommunikation (se vidare avsnitt 2.2.3 om bestämmelserna i Europakonventionen). Lagrådet pekar vidare på att det globala nätet är uppbyggt på ett sådant sätt att det kan bero på slumpartade förhållanden om en viss kommunikation förmedlas delvis i tråd, delvis trådlöst (se lagrådets yttrande i prop. 2006/07:63 s. 170 ff).

Mot samma bakgrund, dvs. uppbyggnaden av det globala nätet, har 11 september-utredningen ifrågasatt om det rättsläge som i praxis har antagits föreligga är väl förenligt med skyddet i regeringsformen och Europakonventionen (se SOU 2003:32 s. 268 ff). Integritetsskyddskommittén har anfört att nämnda praxis, oavsett hur väl motiverad denna är av historiska eller andra skäl, inger betänkligheter från integritetssynpunkt (se SOU 2007:22 s. 255 f och SOU 2008:3 s. 261 f).

2.2.2 Behovet av lagstöd för avlyssning i tråd

Till skillnad från vad som hittills har gällt för elektronisk kommunikation i etern har inhämtning av signaler i tråd alltid ansetts vara av synnerligen integritetskänslig natur och omfattas tveklöst av skyddet i 2 kap. 6 § regeringsformen och Europakonventionen.

Sådan avlyssning har därför omgärdats av särskilda regelsystem för att förhindra missbruk, t.ex. genom bestämmelser om hemlig teleavlyssning och hemlig teleövervakning i 28 kap. rättegångsbalken.

2.2.3 Europakonventionen

Av Europakonventionens artikel 8.1 följer att var och en har rätt till skydd för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Europakonventionen gäller sedan år 1995 som svensk lag.

Med korrespondens avses olika former för att överföra meddelanden mellan individer. Så omfattas exempelvis meddelanden med hjälp av telefon, telefax, radio och datorer av konventionens skydd (se Danelius, Mänskliga rättigheter i europeisk praxis, 2007, s. 344).

Inskränkningar i de angivna rättigheterna får ske under vissa förutsättningar. En inskränkning måste enligt artikel 8.2 ske med stöd av lag och inskränkningen ska vara ägnad att tillgodose något av de syften som anges i artikeln. Som exempel kan nämnas statens säkerhet, den allmänna säkerheten och förebyggande av oordning eller brott. Inskränkningen måste anses vara nödvändig i ett demokratiskt samhälle och vara utformad med en sådan precision att inskränkningen av rättigheten är i rimlig utsträckning förutsebar.

Av intresse i sammanhanget är också innehållet i artikel 13 i konventionen. Av bestämmelsen framgår att var och en som anser sig ha fått sina fri- och rättigheter kränkta ska ha tillgång till ett effektivt rättsmedel inför en nationell myndighet.

Signalspaning har varit föremål för Europadomstolens bedömning. Två avgöranden i domstolen är av särskilt intresse: Weber och Saravia mot Tyskland år 2006 (54934/00) samt Liberty m.fl. mot Storbritannien år 2008 (58243/00).

I fallet Weber och Saravia mot Tyskland prövades huruvida signalspaning som bedrevs av den tyska underrättelsetjänsten Bundesnachrichtendienst stod i överensstämmelse med framför allt artikel 8 i Europakonventionen. Övervakningen var av generell, strategisk natur (strategic monitoring) och syftade till att identifiera allvarliga hot mot landets säkerhet såsom väpnade attacker eller internationell terrorism och vissa andra allvarliga brott. Domstolen fann att avlyssningen omfattades av skyddet i artikel 8.1 och att rättigheter enligt den artikeln hade kränkts. Domstolen fann emellertid vidare att avlyssningen hade skett i enlighet med tysk lag och att den tyska lagstiftningen uppfyllde de krav som framgår av artikel 8.2. I

målet framförde klagandena också den invändningen att Tyskland genom övervakningen skulle kränka andra länders suveränitet. Domstolen fann att eftersom övervakningen genomfördes med utrustning på tyskt territorium och den information som inhämtades användes i Tyskland kunde någon sådan kränkning inte anses ha ägt rum.

Även i fallet Liberty m.fl. mot Storbritannien prövades signalspaning i form av övervakning på strategisk nivå. Domstolen fann även i detta fall att rättigheter som omfattas av artikel 8.1 hade kränkts. Domstolen ansåg emellertid inte att den lagstiftning som låg till grund för avlyssningen uppfyllde kraven i artikel 8.2. Domstolen menade bl.a. att det inte av lagstiftningen framgick med tillräcklig tydlighet vilken övervakning och kontroll som fanns kring avlyssningen samt under vilka förutsättningar det material som samlades in kunde användas, bevaras och förstöras. Vid tiden för den avlyssning som var föremål för domstolens prövning reglerades den typen av frågor inte i en offentlig lagtext, utan den ansvarige ministern hade i uppgift att vidta de åtgärder han fann nödvändiga för att försäkra sig om att det material som inhämtades inte missbrukades. Domstolen menade att regler för hur det insamlade materialet kunde användas och bevaras skulle fastställas på ett sätt som allmänheten kunde ta del av.

I fallet Liberty m.fl. mot Storbritannien klargjorde domstolen också att den inte finns skäl att tillämpa olika principer på strategisk övervakning av telekommunikationer och övervakning som inriktas på enskilda individers kommunikation.

2.3 Signalspaning och hemlig teleavlyssning – skillnader och likheter

För att rätt kunna bedöma behovet av signalspaning inom Säkerhetspolisen och den övriga polisen måste klargöras vilka skillnader och likheter signalspaningen har jämfört med de straffprocessuella tvångsmedel som finns att tillgå.

De straffprocessuella tvångsmedel som är aktuella att jämföra med är hemlig teleövervakning och hemlig teleavlyssning. De båda tvångsmedlen regleras i 27 kap. 18–30 §§ rättegångsbalken. Likheterna kan tyckas särskilt stora i och med att signalspaning numer inom ramen för försvarsunderrättelseverksamheten kan ske också i trådburen trafik. Det är därmed såvitt gäller signalspaning i tråd främst

användningsområdet som skiljer den metoden från exempelvis hemlig teleavlyssning, inte vilken typ av kommunikationer som är möjliga att avlyssna. Som jag anfört inledningsvis (avsnitt 1.2.2) blir begreppet signalspaning därmed framför allt en beteckning som avser den övervakning av telekommunikationer som utförs av Försvarets radioanstalt på olika myndigheters uppdrag, inte en beteckning för en särskild teknik eller för övervakning av en särskild typ av kommunikation.

Med hemlig teleavlyssning avses att telemeddelanden som har befordrats till eller från ett telefonnummer, en kod eller annan teleadress, i hemlighet avlyssnas eller tas upp för återgivning av innehållet i meddelandet. Hemlig teleövervakning innebär att uppgifter i hemlighet hämtas in om telemeddelanden som befordras eller har befordrats till eller från en viss teleadress eller att sådana meddelanden hindras från att nå fram.

Användningen av hemlig teleövervakning och hemlig teleavlyssning förutsätter att en förundersökning har inletts. En förundersökning förutsätter i sin tur att det finns anledning att anta att ett brott har begåtts (23 kap. 1 § rättegångsbalken).

Förutsättningarna för att få använda hemlig teleavlyssning är att förundersökningen gäller brott för vilket inte är föreskrivet lindrigare fängelsestraff än två år, samt försök förberedelse eller stämpling till sådant brott om en sådan gärning är belagd med straff. Hemlig teleavlyssning får vidare användas vid en förundersökning angående annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Hemlig teleövervakning får användas vid förundersökning angående brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader och för vissa särskilt angivna brott i övrigt.

Hemlig teleövervakning och hemlig teleavlyssning förutsätter vidare att det inom ramen för förundersökningen finns en skäligen misstänkt person. Åtgärden måste också bedömas vara av synnerlig vikt för utredningen.

Det måste finnas en känd teleadress som kan övervakas eller avlyssnas. Teleadressen måste innehas eller ha innehafts av den skäligen misstänkte personen eller annars kan antas ha använts eller komma att användas av den misstänkte. Det är också möjligt att avlyssna eller övervaka en annan teleadress som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta.

Tillstånd till hemlig teleavlyssning och hemlig teleövervakning meddelas av rätten på ansökan av en åklagare. Tiden för avlyssningen eller övervakningen får inte bestämmas längre än nödvändigt och får, såvitt gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.

I rättegångsbalken finns vidare bestämmelser kring granskningen av det material som erhålls vid hemlig teleavlyssning och hemlig teleövervakning, om bevarandet av sådant material och om i vilka fall materialet ska förstöras samt om användningen av eventuell överskottsinformation. Det finns i bestämmelserna vidare ett absolut förbud mot att avlyssna samtal mellan den misstänkte och hans eller hennes försvarare. Slutligen finns, såvitt gäller hemlig teleavlyssning, bestämmelser om s.k. offentliga ombud, vars uppgift är att i samband med rättens prövning tillvarata enskildas integritetsintressen.

Även i lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott finns bestämmelser om användningen av hemlig teleavlyssning och hemlig teleövervakning. Bestämmelserna i lagen innebär dels att hemlig teleavlyssning och hemlig teleövervakning i vissa fall kan användas även om det för brottet inte är föreskrivet så långa fängelsestraff som framgår ovan, dels att åklagare i vissa brådskande fall kan besluta om avlyssning eller övervakning i avvaktan på rättens beslut. Lagen gäller endast för vissa särskilt angivna brott.

Såväl hemlig teleavlyssning som hemlig teleövervakning kan också användas i preventivt syfte. Enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott kan hemlig teleavlyssning och hemlig teleövervakning användas om det finns särskild anledning att anta att en person kommer att utöva viss allvarlig brottslig verksamhet. Även om åtgärden således kan vidtas utan att en förundersökning har inletts, dvs. utan att det finns misstanke om att det har begåtts ett konkret brott, krävs att en misstänkt individ har identifierats och att dennes teleadress är känd.

Det finns möjligheter att låta verkställa en hemlig teleövervakning eller en hemlig teleavlyssning utanför Sveriges gränser. Tvångsmedlen kan i vissa fall med stöd av lagen (2000:562) om internationell rättslig hjälp i brottmål verkställas i andra länder med hjälp av det landets myndigheter. I många fall, särskilt i vårt närområde, kan en sådan begäran från svenska myndigeter verkställas både snabbt och effektivt. Den möjligheten står emellertid självfallet inte till buds i världens alla länder och en sådan begäran skulle

framstå som orimlig i de fall det är myndigheterna i det land där den misstänkte befinner sig som står bakom den brottsliga verksamheten i Sverige, t.ex. olovlig underrättelseverksamhet.

2.4 Vissa begränsningar i användningen

I syfte att skydda Försvarets radioanstalts arbetsmetoder och förmåga finns begränsningar i hur Säkerhetspolisen och den övriga polisen kan använda de underrättelserapporter som Försvarets radioanstalt redovisar.

Försvarets radioanstalt ställer undantagslöst kravet att innehållet i rapporterna inte får offentliggöras utan myndighetens medgivande. Begränsningen innebär att underrättelserapporterna inte utan medgivande från Försvarets radioanstalt kan ingå i en förundersökning och inte heller kan användas som bevisning i en domstol.

Inte heller kan Säkerhetspolisen eller den övriga polisen utan Försvarets radioanstalts medgivande använda materialet i ett internationellt samarbete.

3 Polisens signalspaning – från andra världskriget fram till i dag

3.1 Inledning

Signalspaning har under lång tid varit en viktig inhämtningsmetod för Säkerhetspolisen och dess föregångare inom polisorganisationen.

Spaningen har bedrivits både i form av fjärrspaning och närspaning och har utförts såväl av den egna organisationen som med stöd av Försvarets radioanstalt.

Signalspaningen har därtill över åren skiftat fokus, från en metod som inledningsvis enbart användes som stöd för kontraspionageverksamheten till en mer generellt använd metod.

3.2 Den s.k. agentradiospaningen

3.2.1 Polisens signalspaningsorganisation

Hösten 1939, när andra världskriget hade inletts, inrättades en första s.k. radiokontrollenhet inom polisens säkerhetstjänst. Verksamheten byggdes ut under krigsåren och har bedömts som relativt framgångsrik. Syftet med verksamheten var begränsad till att uppdaga agentradiosändningar, dvs. radiosändningar till och från utländska agenter i Sverige.

Vid krigsslutet ifrågasattes om verksamheten skulle bedrivas vidare eller inte. Regeringen beslutade år 1946 att verksamheten skulle fortsätta under ledning av dåvarande Statspolisen, om än i begränsad omfattning. Inriktningen var att signalspaningsorganisationen i huvudsak skulle vara en beredskapsorganisationen, varför personalstyrkan skars ned.

Under mitten av 1950–talet väcktes frågan om att överföra verksamheten till Försvarets radioanstalt. Det konstaterades emellertid

att den signalspaning som bedrevs till övervägande del var polisiär och att den därför borde vara kvar inom polisen.

Verksamheten bedrevs under dessa år i en mycket begränsad omfattning och polisen tappade kompetens på området i takt med att nya metoder för överföring av meddelanden utvecklades.

Inställningen till polisens signalspaning svängde efter hand och det klargjordes under 1960–talet att signalspaning och den efterföljande bearbetningen av den information man inhämtade var nödvändig även i fredstid.

Verksamheten bytte namn och hemvist inom polisen genom åren och kom under 1970–talet att organiseras som en egen rotel vid dåvarande säkerhetsavdelningen vid Rikspolisstyrelsen. Roteln organiserades centralt, regionalt och lokalt och kom att sysselsätta drygt 80 medarbetare. Verksamheten kom även att utgöra en beredskapsorganisation.

3.2.2 Metod och syfte

Syftet med *fjärrspaningen* var under hela den tid som verksamheten organiserades inom polisen, dvs. fram till början av 1990–talet, att avlyssna och kartlägga agentradiotrafik från utlandet. Signalspaningen var således ett verktyg som uteslutande användes inom kontraspionaget.

Främmande makt kommunicerade med sina agenter i Sverige via kortvåg. Sändningarna var huvudsakligen s.k. enkelriktade sändningar, dvs. de mottogs av en agent i Sverige men denne svarade inte utan hade att agera i enlighet med de instruktioner som framgick av sändningen. Radiotrafiken kunde innehålla instruktioner eller andra meddelanden från uppdragsgivaren utomlands till agenterna i Sverige, ofta kodat i form av sifferkombinationer.

Genom att avlyssna sändningarna från avsändare i andra länder gavs möjlighet att dels identifiera avsändaren, dels lokalisera i vilket geografiskt område mottagaren befann sig. Mottagaren kunde inte lokaliseras med någon större precision, men kunde i vart fall avgränsas exempelvis till Mälardalsområdet eller en annan motsvarande region. Genom spaningen kunde säkerhetstjänsten således få kunskap om dels från vilka länder radiotrafiken sändes, dels det antal mottagare i Sverige som trafiken riktade sig till och ungefär var i Sverige dessa befann sig. I den mån man lyckades tyda innehållet i meddelandena fick man självfallet ytterligare kunskap.

Syftet med signalspaningen var därmed inte i första hand att avslöja enskilda individers placering eller deras enskilda planer. För det syftet fanns mer effektiva spaningsmetoder. I stället var avsikten framför allt att försöka få en uppfattning om underrättelseverksamhetens omfattning och intensitet.

Inom ramen för fjärrspaningen kunde polisen också avlyssna radiotrafik som inte riktade sig mot en mottagare Sverige, men som var hörbar även i Sverige.

Syftet med *närspaningen* var framför allt att avlyssna radiotrafik från de utländska agenterna i Sverige till deras uppdragsgivare utomlands eller till andra agenter i Sverige. Om ett sådant radiomeddelande avlyssnades kunde avsändaren i Sverige lokaliseras med relativt stor precision. Närspaning genomfördes ofta med mobila enheter i syfte att med en än bättre precision lokalisera avsändaren.

3.2.3 Översyn av verksamheten

Interna översyner

Rikspolisstyrelsen lät under 1980–talet genomföra två översyner av sin signalspaningsverksamhet.

I den ena översynen behandlades främst interna, organisatoriska frågor. Frågan att överföra verksamheten till Försvarets radioanstalt berördes kort, men utredaren avfärdade tanken med motiveringen att en sådan förändring inte skulle gagna polisen och dess uppdrag.

I den andra översynen behandlades frågan om ett samarbete mellan polisen och Försvarets radioanstalt på ett djupare plan. Polisen och Försvarets radioanstalt var överens om att den teknologiska utvecklingen var accelererande och kostnadskrävande och att det därför var angeläget att tillvarata möjligheterna till samarbete och samverkan i syfte att minska myndigheternas resursbehov avseende utveckling, anskaffning och drift av signalspaningssystem. Liksom i den tidigare översynen avfärdades en sammanslagning av de båda myndigheternas signalspaningsverksamhet med motiveringen att polisens signalspaning var att betrakta som en rent polisär verksamhet.

Säpo-kommittén

Regeringen tillsatte år 1987 en kommitté under ambassadören Carl Lidboms ledning i syfte att genomföra en allmän översyn av Säkerhetspolisen, den s.k. Säpo-kommittén.

Beträffande Säkerhetspolisens signalspaning anförde kommittén i ett betänkande år 1988 att inriktningen för framtiden borde vara en mer långtgående samverkan mellan Säkerhetspolisen och Försvarets radioanstalt i teknik- och metodfrågor (SOU 1988:16 s. 182 ff).

Ställningstagandet motiverades med att det enligt kommitténs mening fanns skäl att även i fortsättningen bedriva signalspaning för Säkerhetspolisens räkning. Kommittén konstaterade emellertid att kostnaderna för fjärrspaningen var stora och att verksamheten samtidigt var för liten för att i längden kunna hålla jämna steg med utvecklingen på radioteknikens område.

Myndigheterna borde därför enligt kommittén i fortsättningen bedriva utvecklingsarbete i samverkan med varandra där Försvarets radioanstalt borde svara för huvuddelen av den tekniska kompetensen medan Säkerhetspolisen i första hand skulle bidra med polisiär sakkunskap. Upphandlingen av signalspaningsmateriel borde ske gemensamt för de båda myndigheterna, lämpligen så att Försvarets radioanstalt skulle äga materielen och ställa den till Säkerhetspolisens förfogande. En samlokalisering borde enligt kommittén vidare ske vad gällde Säkerhetspolisens och Försvarets radioanstalts signalspaningsstationer, både i Stockholm och på andra orter.

Kommittén föreslog mot denna bakgrund att regeringen skulle uppdra åt Rikspolisstyrelsen och Försvarets radioanstalt att undersöka förutsättningarna för en ökad samverkan.

3.2.4 Försvarets radioanstalt övertar Säkerhetspolisens fjärrspaning

Mot bakgrund av bl.a. Säpo-kommitténs överväganden och rekommendationer övertog Försvarets radioanstalt i början av 1990–talet successivt fjärrspaningen från Säkerhetspolisen. Försvarets radioanstalt drev därefter verksamheten vidare på polisens uppdrag. Säkerhetspolisen avvecklade samtidigt sin egen fjärrspaningsverksamhet.

Inom Säkerhetspolisen behöll man bearbetningen av den information som Försvarets radioanstalt hämtade in genom fjärrspaningen. Försvarets radioanstalt hade således, såvitt gäller den del av signalspaningen som nu har redogjorts för, huvudsakligen att utföra den tekniska inhämtningen och att vidarebefordra den information man hämtat in till Säkerhetspolisen.

Den här beskrivna uppdragsverksamheten avseende den s.k. agentradiotrafiken har på Säkerhetspolisens initiativ numer upphört. Verksamheten har inte återupptagits vid Säkerhetspolisen.

Säkerhetspolisen behöll vidare närspaningen inom den egna organisationen. Den verksamheten bedrivs i dag i en mycket ringa omfattning och har haft sin största användning vid tillfällen då Säkerhetspolisen biträtt Rikskriminalpolisen och polismyndigheterna med närspaning.

3.3 Försvarets radioanstalts stöd till Säkerhetspolisen och Rikskriminalpolisen i övrigt

Försvarets radioanstalt har – utöver spaningen avseende agentradiotrafiken – allt sedan andra världskriget biträtt polisen och Säkerhetspolisen med underrättelseinhämtning genom signalspaning.

Fram till 1970–talet inskränkte sig biträdet till kontraspionageverksamheten inom Säkerhetspolisen. Under 1970–talet utökades biträdet till att avse också stöd till Säkerhetspolisens kontraterrorismverksamhet och under 1990–talet till att även avse Säkerhetspolisens arbete kring spridning av massförstörelsevapen.

Försvarets radioanstalt har också sedan 1990–talet biträtt Rikskriminalpolisen med signalspaning avseende grov organiserad brottslighet. Den verksamheten har emellertid haft en tämligen begränsad omfattning. Rikskriminalpolisen har fungerat som beställare och kontaktpunkt gentemot Försvarets radioanstalt för hela den vanliga polisorganisationen, dvs. även för de 21 polismyndigheterna.

Försvarets radioanstalt har därtill sedan andra världskriget biträtt såväl Säkerhetspolisen som Rikskriminalpolisen med tekniskt stöd i form av exempelvis kryptoforcering.

Resultatet av Försvarets radioanstalts arbete redovisas till Säkerhetspolisen och Rikskriminalpolisen i form av rapporter. Rapporternas innehåll skiftar självfallet beroende på vilken typ av information uppdragsgivaren, dvs. Säkerhetspolisen eller Rikskriminalpolisen, har efterfrågat. Det kan röra sig om dels kortfattade rapporter om

enskilda händelser (såsom innehållet i ett meddelande samt uppgifter om avsändare och mottagare), dels s.k. trafikkartläggningar (dvs. omfattande beskrivningar av trafikmönster). Andra typer av rapporter till Säkerhetspolisen och Rikskriminalpolisen är rapporter av strategisk natur kring olika internationella företeelser och händelseförlopp.

3.4 Nya förutsättningar för Försvarets radioanstalts verksamhet

Grunden för Försvarets radioanstalts biträde till Säkerhetspolisen och den övriga polisen var tidigare att Försvarets radioanstalt enligt sin instruktion hade i uppgift att bedriva signalspaning på uppdrag av regeringen, Försvarsmakten och övriga uppdragsgivare. Såväl Säkerhetspolisen som Rikskriminalpolisen hade därvid såsom övriga uppdragsgivare möjlighet att inrikta Försvarets radioanstalts verksamhet mot sina egna intresseområden (se den numer upphävda 1 § förordningen [1994:714] med instruktion för Försvarets radioanstalt).

Den 1 januari 2008 trädde en ändring i Försvarets radioanstalts instruktion i kraft (SFS 2007:937). Förändringen innebär att Försvarets radioanstalt fortsättningsvis enbart ska bedriva sådan verksamhet som omfattas av lagen (2000:130) om försvarsunderrättelseverksamhet (se närmare om den verksamheten i avsnitt 4.1).

Såväl Säkerhetspolisen som Rikskriminalpolisen har, efter bemyndigande av regeringen, hittills haft möjlighet att ange den närmare inriktningen av Försvarets radioanstalts signalspaning, om än begränsad till att avse verksamhet som faller inom ramen för den övergripande inriktning av försvarsunderrättelseverksamheten som regeringen har angett (se 1 § andra stycket lagen om försvarsunderrättelseverksamhet).

Försvarets radioanstalt har därmed sedan den 1 januari 2008 saknat möjlighet att bistå Säkerhetspolisen och övriga polisen med annat än vad som kan anses rymmas inom ramen för försvarsunderrättelöseverksamheten. Det tydliggjordes i det sammanhanget också att Försvarets radioanstalt var förhindrad att bistå Säkerhetspolisen och den övriga polisen med signalspaning i brottsutredande syfte, dvs. spaning inom ramen för en pågående förundersökning (prop. 2006/07:63 s. 108).

Av den överenskommelse mellan allianspartierna som offentliggjordes i september 2008 och som regeringen nu lagt fast i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) framgår att Försvarets radioanstalt fortsättningsvis ska få bedriva signalspaning endast på beställning av regeringen, Regeringskansliet och Försvarsmakten. När det regelverk som följer av överenskommelsen träder i kraft saknas därmed förutsättningar för Försvarets radioanstalt att i någon form och i något syfte biträda Säkerhetspolisen och den övriga polisen med signalspaning.

4 Signalspaning i försvarsunderrättelseverksamheten

4.1 Vad avses med försvarsunderrättelseverksamhet?

4.1.1 Ett nytt och vidgat mandat

Den svenska försvarsunderrättelseverksamheten utvecklades efter andra världskriget. Verksamheten präglades av den hotbild som var helt dominerande under det kalla kriget, dvs. ett yttre militärt hot från en annan stat eller grupp av stater.

Försvarsunderrättelseverksamheten är reglerad i lagen (2000:130) om försvarsunderrättelseverksamhet. Den nu gällande definitionen av försvarsunderrättelseverksamhet trädde i kraft den 1 oktober 2007 (SFS 2007:664).

Försvarsunderrättelseverksamheten definieras numer som en verksamhet som ska ”bedrivas till stöd för svensk utrikes-säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet”. Vidare ingår i verksamheten att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Verksamheten avser endast utländska förhållanden (1 §).

Det är alltjämt en viktig uppgift för försvarsunderrättelseverksamheten att bevaka den militära utvecklingen i vårt närområde. Som framgår av den nu gällande definitionen av försvarsunderrättelseverksamhet är emellertid mandatet vidare än att kartlägga yttre militära hot mot landet. Det vidgade mandatet har motiverats med den allt mer komplexa säkerhetspolitiska hotbilden, den tekniska utvecklingen och det ökande svenska engagemanget i internationella insatser. Det har ansetts att en rad andra hot och risker än de traditionella måste ges en ökad uppmärksamhet i säkerhetspolitiken och därmed också i underrätteleverksamheten. Sådana risker och hot är bl.a.

- terrorism,
- spridning av massförstörelsevapen,
- internationell kriminalitet av stor omfattning och kvalificerad art som t.ex. smuggling av vapen, droger eller människor, samt
- hot mot den tekniska infrastrukturen, inte minst tele- och datasystemen.

Utmärkande för denna typ av risker och hot är att de inte sällan utgår från icke-statliga aktörer. De är vidare transnationella och icke-militära samt berör flera samhällssektorer (prop. 2006/07:63 s. 31 ff.).

Centralt i verksamheten är ett internationellt samarbete. De myndigheter som bedriver försvarsunderrättelseverksamhet får därför, efter regeringens närmare bestämmande, etablera och upprätthålla samarbete med andra länder och internationella organisationer.

Försvarsunderrättelseverksamheten bedrivs av Försvarsmakten (genom den militära underrättelse- och säkerhetstjänsten, MUST), Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut.

Det är regeringen som bestämmer försvarsunderrättelseverksamhetens inriktning. Inom ramen för den inriktningen får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten (1 § andra stycket).

4.1.2 Gränsdragning mot den brottsbekämpande verksamheten

Med den vidgade definition av försvarsunderrättelseverksamhet som gäller sedan år 2007 uppkommer frågan om gränsdragning mellan försvarsunderrättelseverksamhet och andra myndigheters verksamhet och ansvarsområden, inte minst den verksamhet som de brottsbekämpande myndigheterna bedriver. Områden som terrorism, spridning av massförstörelsevapen och grov organiserad brottslighet med internationella kopplingar utgör centrala delar av Säkerhetspolisens och den övriga polisens uppdrag.

Regeringen har i den frågan anfört att den tekniska utvecklingen och de gränsöverskridande hoten i praktiken har medfört att skiljelinjen mellan inre/polisiär och yttre/militär säkerhet inte är lika klar som tidigare. En ökande del av den underrättelseinformation som polisen

inhämtar avser utländska förhållanden och Säkerhetspolisens verksamhet utgörs i allt högre grad av underrättelseverksamhet.

Gränsdragningen bör enligt regeringen i första hand göras med beaktande av respektive verksamhets ändamål. Försvarsunderrättelseverksamheten är i första hand inriktad på att ge sådan strategisk information som regeringen och olika myndigheter behöver för planering, beslut och andra åtgärder. Med sådan information kan regeringen och myndigheterna tidigt formulera strategier och politik för att möta olika fenomen som annars kan utvecklas till någon form av kris.

Det utökade mandatet för försvarsunderrättelseverksamheten att ägna uppmärksamhet åt internationell kriminalitet innebär enligt regeringen inte att det är frågan om huruvida en verksamhet är kriminell eller inte som står i fokus. Sådan verksamhet aktualiseras i stället i den mån den kan bedömas ha potential att utgöra ett hot mot landet, oavsett hur den i rättslig mening ska betraktas. I vilken utsträckning ett sådant hot kan mötas med de instrument som de brottsbekämpande myndigheterna förfogar över är enligt regeringen en bedömning som ska göras av dessa myndigheter. Samma information kan hos en annan myndighet, utanför den brottsbekämpande sektorn, läggas till grund för bedömningar av hur hotet ska hanteras i andra avseenden och med metoder som står den myndigheten till buds.

Regeringen har betonat att försvarsunderrättelseverksamheten inte utgör en brottsbekämpande verksamhet. Det råder enligt regeringen ingen tvekan om att användningen av straffprocessuella tvångsmedel och annat utövande av polisiära befogenheter ska vara förbehållna polisen och andra brottsbekämpande myndigheter. Vidare har regeringen klargjort att försvarsunderrättelseverksamheten inte får innefatta förfarande i samband med förundersökning.

Regeringen har samtidigt framhållit vikten av att kartläggning av terrorism och annan internationell brottslighet av sådan kvalificerad art att den kan utgöra ett hot mot landet inte utesluts från tillämpningsområdet för försvarsunderrättelseverksamheten. Inhämtningen av sådana underrättelser får enligt regeringen emellertid inte ske på ett sådant sätt att polisens eller andra brottsbekämpande myndigheters arbete i landet störs eller motverkas. Regeringen har därvid framhållit att signalspaning inte är en inhämtningsmetod som kan störa utövandet av den brottsbekämpande eller brottsförebyggande verksamheten. Regeringen har vidare framhållit att det även i fortsättningen är poli-

sen som ansvarar för att leda och bedriva bekämpningen av sådan kriminalitet (prop. 2006/07:63 s. 43 ff och 135 f).

Gränsdragningen gentemot de brottsbekämpande myndigheternas verksamhet har författningsreglerats i 4 § lagen (2000:130) om försvarsunderrättelseverksamhet.

4.2 Signalspaning i försvarsunderrättelseverksamheten

4.2.1 Bakgrund

Inhämtning av information inom förvarsunderrättelseverksamheten sker antingen personbaserat eller genom teknisk inhämtning. Huvuddelen av det inhämtade råmaterialet inom försvarsunderrättelseverksamheten kommer från signalspaning genom Försvarets radioanstalts försorg.

Signalspaningen har hittills varit begränsad till trådlös kommunikation, dvs. spaning i etern. Fram till 1990-talet överfördes stora mängder kommunikation över längre avstånd oftast helt eller delvis trådlöst, dvs. via radio eller satellit. I dag är förhållandena helt annorlunda. Den helt dominerande delen av den elektroniska kommunikationen sker i stället via kabel. Enligt uppgift från Försvarets radioanstalt går i dag 95 procent av all internationell trafik i kabel och den andelen ökar. I Sverige och vårt närområde är andelen än högre. Möjligheten att via signalspaning i etern inhämta relevanta underrättelser har därför reducerats radikalt.

Signalspaning i etern har, som framgått ovan (avsnitt 2.2), ansetts inte kräva något särskilt lagstöd. Utgångspunkten har varit att etern är fri att avlyssna.

Statsmakterna har konstaterat att för att bevara och stärka underrättelseverksamheten är det nödvändigt att ge signalspaningen tillgång till såväl eter- som trådburen kommunikation. Statsmakterna har samtidigt konstaterat att en sådan förändring kräver förstärkningar av det regelverk som syftar till att skydda den personliga integriteten.

4.2.2 En ny rättslig reglering

Bakgrund

Den 1 januari 2009 trädde lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet i kraft.

Regeringens förslag på ny lagstiftning lades fram för riksdagen i mars 2007 (prop. 2006/07:63). Förslaget behandlades i försvarsutskottet (betänkandet 2006/07:FöU10). Riksdagen beslutade i juni 2007 att förslaget skulle vila i minst ett år.

Försvarsutskottet behandlade ärendet på nytt år 2008 (betänkandet 2007/08:FöU14). Kammaren beslutade den 18 juni 2008 att återförvisa ärendet till försvarsutskottet. Försvarsutskottet återkom samma dag med ett nytt betänkande i ärendet (2007/08:FöU15). Utskottet tillstyrkte regeringens förslag till ny lagstiftning, men valde att komplettera förslaget med förslag till åtgärder i syfte att kringgärda signalspaningen med ytterligare rättssäkerhets- och kontrollmekanismer.

Riksdagen beslutade samma dag att anta utskottets betänkande (rskr. 2007/08:266).

Allmänna förutsättningar för signalspaningen

Av 1 § lagen om signalspaning i försvarsunderrättelseverksamhet framgår att den myndighet som regeringen bestämmer får inom ramen för försvarsunderrättelseverksamheten inhämta signaler i elektronisk form vid signalspaning. Regeringen har samtidigt i förordning angett att det är Försvarets radioanstalt som ska bedriva verksamheten (1 § förordningen [2007:937] med instruktion för Försvarets radioanstalt).

Signalspaning får inte ske annat än om regeringen eller, efter regeringens bestämmande, en myndighet närmare har bestämt inriktningen av signalspaningen.

Försvarets radioanstalt är i sammanhanget en renodlat underrättelseproducerande myndighet. Verksamheten styrs helt av de inriktningar som regeringen och andra myndigheter lämnar till myndigheten. Försvarets radioanstalt initierar således inte inhämtning om det inte föreligger en inriktning som föranleder inhämtningen.

Att inhämtningen enbart får ske inom ramen för försvarsunderrättelseverksamheten innebär att den är begränsad till att avse verksamhet som bedrivs till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Verksamheten

får vidare avse endast utländska förhållanden. I syfte att klargöra tillämpningsområdet anförs i förarbetena till lagen följande.

> Att den verksamhet som regleras i lagen får bedrivas för försvarsunderrättelseändamål innebär att inhämtning t.ex. får ske av uppgifter av relevans för att kartlägga militära hot mot landet och förhållanden som är relevanta för svenskt deltagande i fredsfrämjande och humanitära internationella insatser samt kartläggning under pågående insatser av hot mot svensk personal eller svenska intressen i övrigt. Vidare får inhämtningen avse strategisk kartläggning av internationell terrorism eller annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen. Det är dock inte försvarsunderrättelseverksamhetens uppgift att kartlägga verksamheten i operativt brottsbekämpande syfte.
>
> Andra exempel på ändamål för vilka signalspaning får bedrivas är kartläggning av utveckling och spridning av massförstörelsevapen och krigsmateriel, yttre hot mot samhällets tekniska infrastruktur i form av t.ex. kvalificerade IT-relaterade hot, konflikter utomlands med konsekvenser för internationell säkerhet och internationella företeelser i övrigt av betydelse för svensk utrikes-, säkerhets- och försvarspolitik (prop. 2006/07:63 s. 137).

Inhämtningen får också ske för vissa andra särskilda syften, nämligen 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 signalspaning enligt lagen (1 § andra stycket). Inhämtning med stöd av denna bestämmelse utgör således inte underrättelseverksamhet, utan bedrivs för att tillgodose Försvarets radioanstalts egna behov av teknik- och kompetensutveckling.

Särskilt om inhämtning i tråd

Inhämtning som sker i tråd är i lagen föremål för särskild reglering. Sådan inhämtning får endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör (2 §). Bestämmelsen är avsedd att begränsa signalspaningen till utländska förhållanden, dvs. samma begränsning som följer av att signalspaningen ska ske inom ramen för försvarsunderrättelseverksamheten.

För att inhämtningen ska bli tekniskt möjlig för Försvarets radioanstalt att genomföra följer av en bestämmelse i 6 kap. 19 a § lagen (2003:389) om elektronisk kommunikation ett åliggande för operatörerna att överföra signalerna i sina respektive nät till s.k.

samverkanspunkter. Bestämmelsen har i skrivande stund (juni 2009) ännu inte trätt i kraft.

Av 3 § följer att inhämtning av signaler i tråd ska ske automatiserat och med användning av sökbegrepp. Sökbegreppen ska utformas och användas så att de medför ett så begränsat intrång som möjligt i den personliga integriteten och de får inte vara direkt hänförliga till en viss fysisk person om det inte är av synnerlig vikt för verksamheten.

Inhämtningen ska ske automatiserat av två skäl. För det första är mängden trafik så stor att en rationell inhämtning måste ske automatiserat. För det andra innebär en manuell inhämtning ökade risker för intrång i den personliga integriteten.

Även en automatiserad inhämtning kan emellertid innebära stora intrång i den personliga integriteten, exempelvis om all förekommande trafik skulle lagras för senare bearbetning. En sådan lagring är enligt Försvarets radioanstalt inte möjlig. Användningen av sökbegrepp har därtill ansetts åstadkomma en rimlig avgränsning vad gäller automatiserad inhämtning. Med sökbegrepp avses kombinationer av tekniska 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 utrustning (prop. 2006/07:63 s. 76–77).

Inriktning av verksamheten

Som framgått ovan vad gäller innehållet i 1 § får signalspaning inte ske om inte regeringen, eller den myndighet som regeringen bestämmer, har bestämt inriktningen av signalspaningen. Eftersom signalspaningen ska bedrivas enbart inom ramen för försvarsunderrättelseverksamheten blir konsekvensen att inriktningen av signalspaningen följer inriktningen av försvarsunderrättelseverksamheten i stort.

En särskild bestämmelse gäller emellertid för signalspaningen. Av 4 § följer att en inriktning av signalspaningen inte får avse endast en viss fysisk person. Det konstateras i förarbetena att i vissa fall måste signalspaningen beröra enskildas kommunikationer för att det ska vara möjligt att följa en viss företeelse av relevans för verksamheten. Det framhålls samtidigt att den inte ska inriktas endast mot en enskild utpekad individ, dvs. att kartlägga en viss fysisk person får inte vara det enda syftet med en inriktning.

Tillstånd

För att Försvarets radioanstalt ska kunna verkställa en inriktning av signalspaningen från någon av de myndigheter som har medgetts rätt att inrikta verksamheten krävs enligt 5 § tillstånd. Tillstånd lämnas av en särskild myndighet under regeringen, Signalspaningsnämnden.

Tillstånd får ges endast om inriktningen är förenlig med de syften som anges i lagen om försvarsunderrättelseverksamhet. Ett tillstånd får ges för högst sex månader och får därefter förlängas med högst sex månader i taget.

Tillstånd får lämnas endast om syftet med inriktningen väger klart tyngre än det integritetsintrång som inhämtning i enlighet med inriktningen kan innebära och detta syfte inte kan tillgodoses på ett mindre ingripande sätt. Tillstånd får inte heller lämnas om inriktningen avser endast en viss fysisk person.

Inriktning av signalspaning utan sådant tillstånd får anges endast i brådskande fall, dvs. fall då det skulle medföra allvarliga konsekvenser för väsentliga nationella intressen att avvakta tillståndet. Inriktningen ska då i stället omedelbart anges till Signalspaningsnämnden. Om nämnden skulle finna att inriktningen är sådan att den saknar förutsättningar för tillstånd ska den omedelbart underrätta Försvarets radioanstalt, som därefter omedelbart ska avbryta verksamheten.

Skyldighet att förstöra visst material

Upptagning eller uppteckning av uppgifter som inhämtats genom signalspaning ska enligt 7 § omgående förstöras om innehållet

- berör en viss fysisk person och har bedömts sakna betydelse för försvarsunderrättelseverksamheten,
- avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 och 4 §§ tryckfrihetsförordningen och 2 kap. 3 och 4 §§ yttrandefrihetsgrundlagen (här avses bl.a. identiteten hos författare, meddelare och upphovsmän till skrift eller radioprogram m.m. samt identiteten hos personer som omfattas av det s.k. efterforskningsförbudet),
- rör telefonsamtal eller andra telemedelanden mellan en misstänkt och hans försvarare.

Rapportering

Av 2 § lagen (2000:130) om försvarsunderrättelseverksamhet framgår att försvarsunderrättelseverksamheten ska fullgöras genom inhämtning, bearbetning och analys av information samt att underrättelser ska rapporteras till berörda myndigheter. Sådan rapportering ska därmed även göras med avseende på signalspaningsverksamheten.

Rapporteringen till berörda myndigheter ska ske med den inskränkningen att om uppgifterna berör en viss fysisk person får rapporteringen avse endast förhållanden av betydelse för försvarsunderrättelseverksamheten (8 § lagen om signalspaning i försvarsunderrättelseverksamhet).

Insyn och kontroll

Försvarets underrättelsenämnd ska kontrollera att bestämmelserna i lagen följs.

Nämnden får i sin tillsynsverksamhet bestämma att viss inhämtning ska upphöra eller att viss upptagning eller uppteckning ska förstöras, om det framkommer att inhämtningen står i strid med lagen eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten.

Vidare ska vid Försvarets radioanstalt finnas ett råd med uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten. Rådet ska rapportera sina iakttagelser till Försvarets radioanstalts ledning och, i förekommande fall, till Försvarets underrättelsenämnd.

4.2.3 Riksdagens tillkännagivande och den politiska överenskommelsen

I samband med riksdagens slutbehandling av propositionen En anpassad försvarsunderrättelseverksamhet (prop. 2006/07:63) tillkännagav riksdagen som sin mening vad Försvarsutskottet anfört om ytterligare rättssäkerhets- och kontrollmekanismer. Försvarsutskottet anförde i denna del följande (bet. 2007/08:FöU15 s. 2).

Utskottet anser att regeringen ska meddela närmare föreskrifter i förordningsform om ytterligare rättssäkerhets- och kontrollmekanismer när det gäller

– en precisering av för vilka ändamål signalspaning ska få bedrivas inom ramen för den föreslagna lagstiftningen,

– hur tillämpningen av tillståndsgivningen (inriktning, behov, proportionalitetsbedömning, uppdragsgivare och sökord) ska ske,

– hur förstöring av uppgifter ska genomföras.

Utskottet anser att lagen om signalspaning ska kompletteras på följande sätt:

– att tillstånden enligt signalspaningslagen beslutas av en ny domstolsliknande nämnd,

– att den domstolsliknande nämnden ska fatta beslut om tillstånd för användande av sökbegrepp hänförliga till fysiska personer,

– att regeringen och Regeringskansliet ska ta integritetshänsyn vid sina beslut om inriktningen.

Utskottet anser att regeringen senast under hösten 2008 ska återkomma med förslag till ändringar i signalspaningslagen i dessa delar.

Därutöver ska regeringen

– lämna årliga rapporter till riksdagen,

– redovisa en kontrollstation 2011.

Enligt utskottet ska vidare ett särskilt uppdrag lämnas till Datainspektionen om att fram till kontrollstationen 2011 följa FRA:s verksamhet ur ett integritetsskyddsperspektiv. Till Datainspektionen ska en särskild referensgruppknytas, med personer som nomineras av riksdagspartierna. Regeringen ska också tillsätta en kommitté som utifrån ska följa FRA:s verksamhet generellt från ett integritetsperspektiv fram till kontrollstationen. Kommittén ska bestå av parlamentariker. Kommittén ska tillsätta ett integritetsombud, som har till uppgift att vid tillståndsprövningen bevaka integriteten för personer bosatta i Sverige.

Därefter träffades under hösten 2008 en politisk överenskommelse mellan de partier som ingår i regeringen i syfte att ytterligare – dvs. utöver vad som följer av riksdagens tillkännagivande – förstärka integritetsskyddet. Överenskommelsen presenterades i punktform enligt följande.

1. De ändamål för vilka signalspaning får bedrivas preciseras ytterligare och anges i lag i stället för i förordning.
2. Tillstånd till signalspaning ska prövas av domstol.
3. FRA ska ansöka om tillstånd för all signalspaning. Även signalspaning för regeringens behov omfattas alltså av tillståndskrav.
4. FRA ska bara få tillgång till de "trafikstråk" som domstolen bestämmer.
5. I lagen tydliggörs att FRA inte får signalspana mot trafik med både avsändare och mottagare i Sverige.
6. FRA får endast bedriva signalspaning på beställning av regeringen, Regeringskansliet och Försvarsmakten.

7. En utredning ska tillsättas för att se över polis och Säkerhetspolisens behov av underrättelser.
8. Sökbegrepp som är direkt hänförliga till en viss fysisk person får inte användas utan särskilt tillstånd.
9. Närmare föreskrifter om förstöring meddelas. I lagen tas in en hänvisning till den lagstiftning som reglerar FRA:s personuppgiftsbehandling.
10. Kontrollmyndighetens självständighet och förutsättningar för rättslig efterhandskontroll förstärks.
11. En underrättelseskyldighet till enskild införs.
12. Kontrollmyndigheten ska på begäran av enskild vara skyldig att undersöka om verksamhet avseende honom eller henne har skett i enlighet med lag.
13. Om information från själavårdande samtal skulle komma till FRA måste den omedelbart förstöras.
14. Inget råmaterial (i debatten benämnd trafikdata) får sparas i mer än ett år (ej heller av historiska, statistiska eller liknande skäl).
15. Vid kontrollstationen 2011 ska kontrollorganen göra en bedömning av huruvida FRA:s verksamhet bedrivits på ett etiskt riktigt sätt.

4.2.4 Åtgärder från regeringens sida

Regeringen beslutade den 20 november 2008 förordningen (2008:923) om signalspaning i försvarsunderrättelseverksamhet och ändringar i förordningen (2000:131) om försvarsunderrättelseverksamhet. Regeringen har klargjort att den därmed uppfyllt vad riksdagen tillkännagivit om föreskrifter i förordning.

Den 12 februari 2009 beslutade regeringen om direktiv till en parlamentarisk kommitté med uppdrag att följa tillämpningen av lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (dir. 2009:10) och gav samma dag Datainspektionen i uppdrag att följa personuppgiftsbehandlingen hos Försvarets radioanstalt. Regeringen har klargjort att den därmed tillgodosett vad riksdagen uttalat i fråga om uppföljning av lagstiftningen.

4.2.5 Promemorian Förstärkt integritetsskydd vid signalspaning

Försvarsdepartementet presenterade kring årsskiftet 2008/09 promemorian Förstärkt integritetsskydd vid signalspaning (Ds 2009:01). Promemorian innehöll bl.a. förslag till en rad ändringar i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Syftet

med förslagen var att tillgodose vad riksdagen tillkännagivit och vad partierna i regeringen kommit överens om i sådana frågor som kräver ändring i lag.

Promemorian har remissbehandlats.

4.2.6 Propositionen Förstärkt integritetsskydd vid signalspaning

Regeringen överlämnande den 20 maj 2009 propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) till riksdagen. I propositionen behandlas de förslag till förändringar till följd av den politiska överenskommelsen som kräver lagändring. Förslagen i propositionen överensstämmer i allt väsentligt med innehållet i den ovan nämnda promemorian. Propositionen innehåller i huvudsak följande.

Regeringen föreslår att det i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska framgå att signalspaning i försvarsunderrättelseverksamhet endast ska få bedrivas i syfte att kartlägga:

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
5. allvarliga yttre hot mot samhällets infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen, eller
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- och försvarspolitik.

Vidare föreslås att signalspaning i försvarsunderrättelseverksamhet ska få inriktas endast av regeringen, Regeringskansliet och Försvarsmakten. Regeringen föreslår också att begränsningen av signalspaningen till trafik mellan avsändare och mottagare som inte båda befinner sig i Sverige tydliggörs.

I syfte att säkerställa att signalspaning endast avser kommunikation som är relevant för verksamheten föreslår regeringen att tillgång till signaler i tråd endast ska ges till sådana signalbärare som omfattas av

tillstånd. Tillståndsprövningen ska vidare avse den användning av sökbegrepp som aktualiseras vid inhämtningen.

Tillstånden föreslås av regeringen prövas av en ny domstol, Försvarsunderrättelsedomstolen, på ansökan av signalspaningsmyndigheten. Vid prövningen i domstolen föreslås integritetsskyddsombud närvara.

Skyldigheten att förstöra inhämtad information föreslås utvidgas till att gälla också uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla sådana uppgifter för ändamål som anges i lagen.

Regeringen föreslår vidare att en enskild ska underrättas om det vid signalspaning har använts sökbegrepp som är direkt hänförliga till honom eller henne, såvida inte sekretess gäller för uppgiften. Vidare föreslås att enskilda får rätt att till kontrollmyndigheten anmäla om de anser sig ha varit föremål för otillåten signalspaning. Kontrollmyndigheten föreslås i sådana ha fall ha en skyldighet att utreda detta.

Propositionen har i skrivande stund (juni 2009) ännu inte varit föremål för riksdagens behandling.

5 Användningsområden för signalspaning inom polisen

5.1 Allmänna utgångspunkter

Följande redogörelse för de olika användningsområden för signalspaning som finns vid Säkerhetspolisen och Rikskriminalpolisen bygger i huvudsak på beskrivningar från respektive myndighet.

Det medför självfallet svårigheter att i en offentlig publikation i detalj beskriva uppdrag och arbetsmetoder i framför allt Säkerhetspolisens verksamhet. Framgången i verksamheten bygger i mycket på att myndighetens prioriteringar, kunnande och metoder inte avslöjas för dem som är föremål för myndighetens intresse. En allt för stor grad av öppenhet skulle avsevärt försvaga Säkerhetspolisens förmåga att motverka säkerhetshot. Därtill ska läggas att verksamheten i inte ringa utsträckning förutsätter ett samarbete med myndigheter i andra länder, vilket gör en detaljerad beskrivning än svårare och mer känslig.

Samtidigt måste skapas en insikt om vad signalspaning kan användas till inom såväl Säkerhetspolisen som Rikskriminalpolisen och vilken nytta myndigheterna har av sådan spaning. Redogörelsen nedan utgör en avvägning mellan dessa båda intressen.

5.2 Användningsområden i Säkerhetspolisens verksamhet

5.2.1 Säkerhetspolisens uppdrag och verksamhet

En i allt väsentligt brottsförebyggande verksamhet

Säkerhetspolisens uppdrag är att avslöja brott mot rikets säkerhet, bekämpa terrorism och skydda den centrala statsledningen. Säkerhetspolisen utgör en del av den svenska polisen och i uppdraget ingår att utreda brott. Myndigheten har för att fullgöra den delen av uppdraget polisiära befogenheter.

Tyngdpunkten i Säkerhetspolisens verksamhet är emellertid att i egenskap av Sveriges säkerhetstjänst skydda den centrala statsledningen, bedriva säkerhetsskyddsarbete, samt förhindra brott mot rikets säkerhet och terroristbrott. Verksamheten inriktas efter de hotbilder som finns mot personer eller företeelser som Säkerhetspolisen har i uppdrag att skydda. Hotbilderna bestäms utifrån en bedömning av dels vilken avsikt olika aktörer har att begå brott eller annars orsaka skada, dels vilken förmåga dessa aktörer har att genomföra sina intentioner. Säkerhetspolisen kan med stöd av dessa hotbilder vidta sådana åtgärder att brottslig verksamhet förhindras eller avbryts.

För att skapa en grund för den typ av bedömningar som beskrivs ovan bedriver Säkerhetspolisen säkerhetsunderrättelsetjänst. I underrättelseverksamheten inhämtas information genom olika metoder och från olika källor, t.ex. från öppna källor som är tillgängliga för envar (OSINT – Open Source Intelligence) och från personer (HUMINT – Human Intelligence). Signalspaning (SIGINT – Signal Intelligence) är exempel på ytterligare en sådan metod.

Utmärkande för den typ av säkerhetshotande verksamhet som Säkerhetspolisen har att motverka är att det sällan rör sig om företeelser eller händelser som Säkerhetspolisen uppmärksammas på utifrån, exempelvis genom en anmälan. Säkerhetspolisen har i stället att med egna resurser uppdaga säkerhetshotande verksamhet genom inhämtning av underrättelser.

Verksamhetsområden

Följande verksamhetsområden inom Säkerhetspolisen har särskild relevans i detta sammanhang:

Inom *kontraspionaget* arbetar Säkerhetspolisen med att avslöja spionerі och olovlig underrättelseverksamhet i Sverige. Arbetet bedrivs i huvudsak genom underrättelsearbete som syftar till att inhämta information för att kunna vidta skyddsåtgärder och avslöja eventuella brott. För det fall ett brott avslöjas har Säkerhetspolisen ansvaret att under en åklagares ledning bedriva utredningsarbetet.

Säkerhetspolisen bedriver även *kontraterrorism*. Myndigheten har ansvar för terrorismbekämpningen i Sverige och arbetar framför allt förebyggande genom att förhindra terrorattentat i Sverige eller mot svenska intressen. Uppdraget omfattar vidare att förhindra att terrorattentat utomlands planeras i eller på annat stöds från Sverige. Om ett terrorattentat skulle inträffa i Sverige har Säkerhetspolisen ansvaret för att under en åklagares ledning bedriva utredningsarbetet. Säkerhetspolisen deltar på grund av internationella överenskommelser i det internationella samarbetet mot terrorism och bistår andra länder i deras förebyggande verksamhet och i deras utredningsverksamhet.

Inom *författningsskyddet* arbetar Säkerhetspolisen med att förebygga och avslöja verksamhet som syftar till att med våld, hot eller tvång förändra Sveriges statsskick, påverka myndigheters eller politiska organs beslutsfattande eller hindra medborgare från att utöva sina grundlagsskyddade fri- och rättigheter. Säkerhetspolisen kartlägger och analyserar hot mot samhällsviktiga anläggningar samt kartlägger och motverkar svenska extremistmiljöer som kan utgöra ett hot mot demokratin. Arbetet bedrivs i nära samarbete med landets polismyndigheter. Relativt ny är Säkerhetspolisens inriktning mot s.k. otillåten påverkan, dvs. att kartlägga och motverka trakasserier, hot, våld och korruption som syftar till att påverka förtroendevalda politiker, anställda inom rättsväsendet och företrädare för den fria debatten. Verksamheten är i den delen bl.a. inriktad mot den grova organiserade brottsligheten. Även om det förekommer att Säkerhetspolisen bedriver utredningsarbete med anledning av brott på detta område, består uppdraget i huvudsak av att bistå den vanliga polisen i deras brottsutredningsarbete med sakkunskap och analyser.

Säkerhetspolisen deltar vidare i det s.k. *icke-spridningsarbetet*, dvs. åtgärder som syftar till att förhindra spridning, produktion och anskaffning av massförstörelsevapen. Arbetet går främst ut på att

förhindra att kunskaper, produkter, ämnen eller mikroorganismer förs från eller via Sverige till aktörer som har för avsikt att anskaffa eller vidareutveckla massförstörelsevapen eller deras bärare (dvs. missiler). En stor del av verksamheten handlar om informationsutbyte med såväl internationella organisationer som svenska företag.

Behovet av kunskap om utrikes förhållanden

De typer av hot som Säkerhetspolisen har i uppdrag att uppdaga och avstyra har inte sällan sitt ursprung i utlandet, eller har i vart fall kopplingar till utländska förhållanden. Som exempel kan nämnas att bakom spionerи och olovlig underrättelseverksamhet finns en främmande stat samt att terrorism och spridning av massförstörelsevapen båda är internationella företeelser. Den säkerhetshotande verksamhet som Säkerhetspolisen har i uppdrag att motverka styrs således ofta av aktörer i andra länder.

Samtidigt som Säkerhetspolisens uppdrag nödvändiggör kunskap om utländska förhållanden saknar Säkerhetspolisen befogenheter att agera utanför landets gränser. Myndigheten kan därmed inte själv inhämta uppgifter på plats eller verka preventivt nära ursprunget till den säkerhetshotande verksamheten. I brist på sådana möjligheter blir det viktigt att ha en god uppfattning om de aktörer som initierar och styr verksamheten samt om deras kopplingar till utövare i Sverige.

Utöver de underrättelser som Försvarets radioanstalt rapporterar med avseende på identifierade grupper och individer med kopplingar till ett utländskt förhållande får Säkerhetspolisen regelbundet del av andra underrättelser från Försvarets radioanstalt av mer strategisk natur. Det rör sig exempelvis om iakttagelser kring utvecklingstendenser i olika delar av världen eller om särskilda händelser av betydelse för Sverige och svenska intressen. Den typen av underrättelser är således inte resultatet av en specifik inriktning från Säkerhetspolisen, utan utgör information som Försvarets radioanstalt har inhämtat inom ramen för försvarsunderrättelseverksamheten i övrigt och som bedöms vara av intresse för Säkerhetspolisen.

5.2.2 Exempel på signalspaning i Säkerhetspolisens verksamhet

Säkerhetspolisen har lämnat följande exempel på hur signalspaning skulle kunna ha använts under de hittills gällande förhållandena.

Exempel 1

Säkerhetspolisen har fått uppgifter om att underrättelsetjänsten i X-land har visat ett allt större intresse för norra Europa och det finns tecken som tyder på att X-land bedriver olovlig underrättelseverksamhet i flera länder i vårt närområde.

Säkerhetspolisen riktar signalspaning mot underrättelsetjänsten i X-land och finner att det med viss regelbundenhet skickas meddelanden mellan underrättelsetjänstens huvudkontor och en mottagare i Sverige. Genom signalspaningen kan mottagarens mobiltelefonnummer identifieras. Genom andra typer av spaningsinsatser kan telefonnumret knytas till en individ boende i Stockholm.

Misstankarna om brottslig verksamhet stärks genom ett fortsatt underrättelsearbete och en förundersökning inleds. Säkerhetspolisen har kunnat identifiera en skäligen misstänkt person och har därmed inom ramen för förundersökningen möjlighet att använda straffprocessuella tvångsmedel, t.ex. hemlig teleavlyssning.

Exempel 2

Säkerhetspolisen misstänker att Y-land bedriver olovlig underrättelseverksamhet i Sverige. Vilka personer som bedriver verksamheten i Sverige är oklart, men allt tyder på att den olagliga verksamheten bedrivs av någon tjänsteman vid ett Y-ländskt bolag i Stockholm. På vilket sätt tjänstemannen kommunicerar med sina uppdragsgivare i Y-land är oklart.

Vid signalspaning som riktas mot trafik från bolaget i Stockholm till hemlandet finner man regelbunden trafik till Y-lands underrättelsetjänst. Trafiken kan med hjälp av andra spaningsinsatser knytas till en viss tjänsteman vid bolaget.

Genom ett fortsatt underrättelsearbete stärks misstankarna om att tjänstemannen bedriver brottslig verksamhet. Säkerhetspolisen har därmed kunnat identifiera en skäligen misstänkt person och har

inom ramen för en förundersökning möjlighet att använda straffprocessuella tvångsmedel, t.ex. hemlig teleavlyssning.

Exempel 3

Säkerhetspolisen får av en samarbetande utländsk underrättelsetjänst tips om att det kan finnas personer i Sverige med koppling till en internationell terrororganisation med bas i Q-land. Den utländska underrättelsetjänsten har lyckats identifiera ett svenskt mobiltelefonnummer som har varit i kontakt med höga företrädare för terrororganisationen i Q-land. Mobiltelefonen visar sig vara av kontantkortsmodell och kan därmed inte spåras till någon innehavare.

Genom signalspaning där mobiltelefonnumret används som sökbegrepp avlyssnas flera samtal mellan en person i Sverige och företrädare för terrororganisationen i Q-land. Med hjälp av andra spaningsinsatser kan innehavaren av mobiltelefonnumret identifieras.

Ett fortsatt underrättelsearbete med spaningsinsatser ger Säkerhetspolisen skäl att anta att personen har gjort sig skyldig till terroristbrott. Genom signalspaningen har Säkerhetspolisen således kunnat identifiera en skäligen misstänkt person och har därmed inom ramen för en förundersökning möjlighet att använda straffprocessuella tvångsmedel, t.ex. hemlig teleavlyssning.

Exempel 4

En person i Sverige misstänks för terroristbrott. Förundersökning pågår och personen är föremål för hemlig teleavlyssning.

Genom teleavlyssningen får Säkerhetspolisen kunskap om personens kontakter med en terrororganisation med bas i Z-land. Säkerhetspolisen vet mycket lite om organisationen. Personens kontakter i Z-land identifieras liksom deras mobiltelefonnummer.

Signalspaning riktas mot terrororganisationen i Z-land. Genom spaningen får Säkerhetspolisen kunskap om hur terrororganisationen agerar i en vidare kontext. Kunskapen ökar om hur gruppens medlemmar kommunicerar med varandra, hur verksamheten bedrivs, vad de planerar och vilket intresse som finns från organisationens sida mot vårt närområde. Säkerhetspolisen kan med den kunskapen, i samverkan med myndigheter i de länder som samarbetar i

bekämpningen av internationell terrorism, mer långsiktigt motverka det hot som terrororganisationen utgör.

I den konkreta brottsutredningen kan samtidigt den misstänkte personens verksamhet i Sverige sättas in i ett större sammanhang.

Exempel 5

Från flera samarbetande underrättelsetjänster kommer signaler om att underrättelsetjänsten i P-land bedriver olovlig underrättelseverksamhet mot länder i vårt närområde.

Säkerhetspolisen ser allvarligt på uppgifterna och riktar signalspaning mot P-lands underrättelsetjänst i syfte att undersöka om det sker någon trafik mellan underrättelsetjänsten och individer i Sverige.

Efter genomförd signalspaning – kompletterad med annan underrättelseinhämtning – kan Säkerhetspolisen konstatera att det inte finns några konkreta belägg för att P-land skulle bedriva någon olaglig verksamhet i Sverige.

Exempel 6

En person boende i Sverige misstänks för terroristbrott. Förundersökning pågår och personen är föremål för hemlig teleavlyssning.

Genom teleavlyssningen får Säkerhetspolisen klart för sig att personen har för avsikt att snabbt åka till X-land där den terroristgrupp han misstänks stödja har sin bas. Det finns ingen möjlighet för svenska myndigheter att få den hemliga teleavlyssningen verkställd i X-land.

När den misstänkte personen avreser till X-land sätts signalspaning in med den misstänktes mobiltelefonnummer som sökbegrepp. Genom signalspaningen kan den misstänktes kontakter i X-land följas och hans samröre med terroristorganisationen framstår därmed än tydligare.

5.3 Användningsområden i Rikskriminalpolisens verksamhet

5.3.1 Rikskriminalpolisens uppdrag och verksamhet

Ansvarsområdet

Rikskriminalpolisen är en del av Rikspolisstyrelsen och har, såvitt här är av intresse, ett övergripande ansvar för att bekämpa den grova organiserade brottsligheten.

Den verksamhet som Rikskriminalpolisen bedriver med avseende på den grova organiserade brottsligheten är organiserad vid kriminalpolisenheten. I enheten ingår bl.a. en sektion för kriminalunderrättelsetjänst och analys, en spaningssektion samt en utredningssektion.

Verksamheten är inriktad mot narkotikabrott, illegal invandring, människosmuggling, penningtvätt, miljöbrott, barnpornografi och gängkriminalitet.

Rikskriminalpolisen bedriver i viss utsträckning egna brottsutredningar, men stöder i övrigt lokala polismyndigheter samt utländska och internationella brottsbekämpande organ. Organisationen har särskilt i uppdrag att stödja bekämpningen av brottslighet som är av allvarlig beskaffenhet och har riksomfattande karaktär eller internationell anknytning.

Rikskriminalpolisen är den organisation inom den vanliga polisen som har inriktat Försvarets radioanstalts signalspaning och har därmed stått som såväl beställare som mottagare gentemot Försvarets radioanstalt.

Behovet av signalspaning

Rikskriminalpolisen har inriktat Försvarets radioanstalts signalspaning i en tämligen begränsad omfattning. I de fall signalspaning har använts rör det sig i allt väsentligt om ärenden som har koppling till grov organiserad brottslighet av systemhotande karaktär. Det kan exempelvis röra sig om verksamhet som syftar till att förhindra att vapen från utlandet tillförs gängkriminaliteten i Sverige. En sådan verksamhet kan kräva att information inhämtas utanför Sverige i områden där annan form av inhämtning än signalspaning är svår att använda.

På samma sätt som gäller avseende Säkerhetspolisen får Rikskriminalpolisen också regelbundet tillgång till underrättelser från Försvarets radioanstalt av mer strategisk natur. Den typen av information är således inte resultatet av en specifik inriktning från Rikskriminalpolisen, utan utgör information som Försvarets radioanstalt i övrigt har inhämtat inom ramen för försvarsunderrättelseverksamheten och som bedöms vara av intresse för Rikskriminalpolisen.

5.3.2 Exempel på signalspaning i Rikskriminalpolisens verksamhet

Rikskriminalpolisen har lämnat följande exempel på hur signalspaning skulle kunna ha använts under de hittills gällande förhållandena.

Exempel 1

Underrättelser tyder på att en person boende i X-land styr ett nätverk som bedriver omfattande handel med narkotika och vapen där Sverige är ett av mottagarländerna. Det saknas möjlighet att med hjälp av myndigheterna i X-land begära hjälp med hemlig teleavlyssning eller andra åtgärder mot personen.

Genom signalspaning kan Rikskriminalpolisen få kännedom om personens kontakter med individer i Sverige och utomlands.

Fortsatt underrättelsearbete kan därmed drivas med andra metoder mot nya identifierade misstänkta individer i syfte att samla tillräckligt material för framtida förundersökningar.

Exempel 2

Inhämtade underrättelser tyder på att en person boende i Y-land rekryterar kvinnor under falska premisser att de skall få arbete i Sverige som servitriser eller au-pairflickor. Kvinnorna tvingas sedan till prostitution i Sverige eller andra länder. Underrättelseinformation i Sverige innehåller uppgifter om att vissa personer som reser in i landet är behjälpliga i verksamheten, men informationen räcker inte för att nå upp till graden skälig misstanke. Det saknas möjlighet att med hjälp av myndigheterna i X-land begära hjälp med hemlig teleavlyssning eller andra åtgärder mot personen.

Genom signalspaning kan Rikskriminalpolisen få kännedom om personens kontakter med individer i Sverige och utomlands. Misstänkta kontakter mellan den utpekade huvudmannen i Y-land och personer som reser in i Sverige kan bekräftas.

Fortsatt underrättelsearbete kan därmed drivas med konventionella metoder mot nya identifierade misstänkta individer i syfte att samla tillräckligt material för framtida förundersökningar.

Exempel 3

Inhämtade underrättelser gör gällande en person boende i Z-land tjänar stora pengar på att erbjuda flyktingar resepaket som inkluderar falska dokument, transport samt konsultation vid ansökan om asyl i Sverige. Flera av de personer som köper tjänsterna har gjort så på kredit och tvingas i Sverige till brott eller prostitution för att kunna betala av sin skuld. Underrättelseinhämtning i Sverige har lett till namn på vissa personer i och utanför Sverige som misstänks fungera som mellanhänder och medhjälpare. Ingen information når dock upp till graden skälig misstanke. Det saknas möjlighet att med hjälp av myndigheterna i X-land begära hjälp med hemlig teleavlyssning eller andra åtgärder mot personen.

Genom signalspaning kan Rikskriminalpolisen få kännedom om huvudmannens kontakter med individer i Sverige och utomlands. Misstänkta kontakter mellan den utpekade huvudmannen och personer som reser in i Sverige kan bekräftas.

Detta är till stor hjälp för att kunna inrikta fortsatt underrättelsearbete med konventionella metoder i syfte att samla tillräckligt material för framtida förundersökningar mot identifierade misstänkta individer.

6 En internationell utblick

6.1 Underrättelseverksamhet i ett internationellt perspektiv

6.1.1 Allmänt om underrättelseverksamhet

Underrättelseverksamhet kan generellt beskrivas som en verksamhet som består i att samla in och sammanställa information och att på grundval av det samlade materialet göra olika slags bedömningar. Den metod som används är densamma oavsett inom vilken typ av organisation som verksamheten bedrivs och kan kort beskrivas enligt följande:

- planläggning,
- inriktning,
- inhämtning,
- bearbetning (innefattande analys) och
- delgivning.

Signalspaning utgör i detta sammanhang en inhämtningsmetod bland flera för de myndigheter som bedriver underrättelseverksamhet.

Såvitt här är av intresse bedrivs underrättelseverksamhet i form av underrättelsetjänst, säkerhetsunderrättelsetjänst och kriminalunderrättelsetjänst. Avgränsningarna olika myndigheter emellan kan skilja från land till land.

Underrättelsetjänst bedrivs av en organisation med uppdrag att inhämta underrättelser utanför det egna landet.

Underrättelsetjänster kan vara antingen civila eller militära. Vanligen finns i ett land såväl en civil som en militär underrättelsetjänst, där den militära organisationens uppdrag består i underrättelseverksamhet av militärstrategisk betydelse.

Även inom säkerhetstjänsterna – dvs. de organisationer som har i uppdrag att höja säkerhetsnivån i det egna landet och avslöja hot

som riktas mot landet – bedrivs underrättelseverksamhet och benämns då *säkerhetsunderrättelsetjänst*.

Säkerhetsunderrättelsetjänstens uppgift är att klarlägga säkerhetshotande verksamhet, dvs. brott mot rikets säkerhet (såsom spionerі och olovlig underrättelseverksamhet) och terrorism samt att bedriva författningsskyddande verksamhet.

Säkerhetstjänster finns även inom ramen för militär verksamhet och har då som syfte att skydda den egna militära organisationen mot säkerhetshotande verksamhet.

Den underrättelseverksamhet som bedrivs inom polisen benämns *kriminalunderrättelsetjänst*. Den verksamheten syftar till att klarlägga hotande kriminalitet och ordningsstörningar samt att avslöja kriminella organisationer eller andra brottsliga aktörer.

6.1.2 Myndighetsstrukturen i ett internationellt perspektiv

Tyskland

Bundesnachrichtendienst (BND) är en civil underrättelsetjänst som lyder under förbundsregeringen. Dess övergripande uppdrag är att inhämta och utvärdera information som är av utrikes- och säkerhetspolitisk betydelse för förbundsrepubliken. BND bedriver underrättelseinhämtning utomlands, men kan även inhämta information om utländska förhållanden inom Tyskland och har då möjlighet att använda tvångsmedel. BND har emellertid inga andra exekutiva befogenheter.

Bundesamt für Verfassungsschutz (BfV) är en civil säkerhetsunderrättelsetjänst under inrikesministeriet. Myndigheten har i uppdrag att bedriva författningsskyddande verksamhet, dvs. att inhämta och utvärdera hot mot det demokratiska statsskicket samt förbundsrepublikernas och delstatsrepublikernas bestånd. BfV ska vidare bedriva kontraspionage samt ansvara för säkerhetsskydd och personalkontroll. Myndigheten har inga exekutiva befogenheter, men kan efter tillstånd och under vissa omständigheter använda hemliga tvångsmedel. Varje tysk delstat har en egen myndighet med motsvarande uppdrag som BfV, Landesbehörden für Verfassungsschutz.

Bundeskriminalamt (BKA) är en polisorganisation som lyder under inrikesministeriet och är Tysklands centrala kriminalpolismyndighet. BKA fungerar som nationell kriminalunderrättelse-

tjänst och nationellt samordningsorgan för brottsbekämpning samt som huvudorgan för internationellt polissamarbete. BKA bedriver i viss utsträckning egna brottsutredningar, men bistår annars andra polismyndigheter i deras utredningsverksamhet. Bland BKA:s uppgifter kan nämnas grov organiserad brottslighet, kontraterrorism, Kontraspionage och författningsskydd. Vidare förfogar BKA över en insatsstyrka och en livvaktsstyrka för den centrala statsledningen.

Zentrum für Nachrichtenwesen der Bundeswehr (ZNBw) är den tyska militära underrättelsetjänsten och har som huvudsakligt uppdrag att inhämta underrättelseinformation om militära förhållanden utomlands.

Amt für den Militärischen Abschirmendienst (MAD) är en del av den tyska försvarsmakten och utgör den militära säkerhetstjänsten. Myndigheten har i uppgift att inom Tyskland följa upp och förebygga säkerhetshotande verksamhet som är riktad mot Bundeswehr. Även de platser utomlands där tysk militär är stationerade omfattas av uppdraget. MAD har möjlighet att använda tvångsmedel.

Storbritannien

Secret Intelligence Service (*SIS*, även kallad *MI 6*) är en civil underrättelsetjänst under utrikesministeriet. Dess verksamhet syftar till att bekämpa hot mot den nationella säkerheten och att främja landets utrikes- och försvarspolitik samt ekonomiska välstånd. SIS har i uppdrag att inhämta information om aktiviteter som planeras eller bedrivs av personer som uppehåller sig utanför landet, genomföra andra åtgärder med anledning av sådana aktiviteter samt medverka i att förebygga och uppdaga grov brottslighet.

British Security Service (*BSS*, även kallad *MI 5*) är en civil säkerhetsunderrättelsetjänst under inrikesministeriet. Dess uppdrag är att skydda den nationella säkerheten genom att förebygga hot som uppkommer genom spioneri, terrorism och sabotage samt genom agenter från främmande makt. BSS ska vidare skydda mot handlingar som syftar till att undergräva det centrala parlamentariska statsskicket genom politiska åtgärder, konfliktåtgärder eller med våldsamma medel. BSS ska därutöver bistå landets polismyndigheter i deras verksamhet med att förebygga och uppdaga grov brottslighet. BSS kan använda tvångsmedel i sin verksamhet, men

saknar i övrigt exekutiva befogenheter. Ingripanden som föranleds av verksamheten genomförs i stället av polismyndigheternas s.k. Special Branch-enheter.

Defence Intelligence Staff (DIS) är den centrala militära underrättelsetjänsten i Storbritannien och ingår som en del av försvarsministeriet. Dess uppgift är att inhämta och analysera militär underrättelseinformation.

Nederländerna

Algemene Inlichtingen – en Veiligheidsdienst (AIVD) är en kombinerad civil underrättelsetjänst och civil säkerhetsunderrättelsetjänst som lyder under inrikesministeriet. AIVD bedriver således underrättelseverksamhet såväl inom som utom landets gränser. Myndigheten saknar polisiära befogenheter, men har ett nära samarbete med polisen.

Militaire Inlichtingen – en Veiligheidsdienst (MIVD) är Nederländernas militära underrättelsetjänst och lyder under försvarsministeriet. MIVD bedriver även säkerhetsunderrättelsetjänst såvitt avser förhållanden inom den nederländska försvarsmakten.

6.2 Signalspaning i ett internationellt perspektiv

6.2.1 Inledande kommentarer

Av mina direktiv framgår att jag ska beakta motsvarande system i jämförbara länder. De undersökningar jag har gjort avseende system i andra länder föranleder några inledande kommentarer.

Signalspaning är, liksom underrättelseverksamhet generellt, typiskt sett en hemlig verksamhet. Verksamheten är till sin natur sådan att myndigheternas avsikter och förmåga skyddas från insyn. Detta påverkar självfallet dels möjligheten att studera förhållanden utomlands, dels möjligheten att använda eventuella kunskaper i en offentlig publikation som detta betänkande.

Det kan heller inte uteslutas att en eventuell skepsis till att offentligt diskutera signalspaning till en del har sin grund i den svenska politiska och massmediala debatten kring signalspaning, en debatt som framstår som väl känd bland berörda myndigheter långt utanför Sveriges gränser. Att offentligt diskutera underrättelse-

verksamhet och dess metoder på det sätt som gjorts i Sverige under det gångna året framstår i flera länder som främmande.

Jag har inom ramen för utredningsuppdraget studerat förhållandena i ett flertal jämförbara länder. Resultaten av dessa studier kan sammanfattas i tre olika kategorier:

1. Länder som helt saknar ett offentligt regelverk kring signalspaning.
2. Länder som har ett regelverk kring signalspaning, men där regelverket inte är offentligt eller, till den del det är offentligt, regelverket är tämligen intetsägande.
3. Länder med ett i huvudsak offentligt regelverk och där systemet låter sig beskrivas i en offentlig publikation.

I de länder som helt saknar ett offentligt regelverk bedrivs signalspaningen, såvitt mina studier har visat, enbart i etern och spaningen har där sin legala grund i att etern anses fri att spana i. Det är således samma förhållanden som har rått i Sverige hittills. Gemensamt för de länder i denna kategori som jag har studerat är att de är tämligen ovilliga att över huvud taget offentliggöra att de bedriver sådan spaning och att de i vart fall inte är villiga att i en offentlig publikation låta beskriva detaljer kring sin signalspaningsverksamhet. Mot denna bakgrund låter sig en beskrivning av signalspaningen i dessa länder inte göras.

I den andra kategorin länder är det ingen hemlighet att signalspaning förekommer, men regelverken som styr verksamheten är till stor del hemliga. Även i dessa länder finns därmed en ovilja att offentligt diskutera de möjligheter och begränsningar som finns kring verksamheten, på samma sätt som gäller all underrättelseverksamhet. En beskrivning av verksamheten i dessa länder saknar därmed värde som ett underlag i den fortsatta beredningen av förslagen i detta betänkande.

Jag har mot denna bakgrund valt att närmare beskriva förhållandena i sådana länder som dels har en signalspaningsverksamhet som låter sig beskrivas, dels har ett offentligt regelverk.

6.2.2 Kanada

Signalspaningsmyndigheten

Signalspaning i Kanada bedrivs av Communications Security Establishment (CSE). CSE är en myndighet under det kanadensiska försvarsdepartementet som startade sin verksamhet efter andra världskrigets slut.

CSE:s uppdrag följer av lag (The Anti-terrorism act, chapter 41 section V.1) och är tredelat:

1. Inhämta och bearbeta information från den globala infrastrukturen i syfte att delge underrättelser om utländska förhållanden.
2. Vara ett rådgivande och vägledande organ för att skydda elektronisk kommunikation och infrastruktur av betydelse för den kanadensiska staten.
3. Ge tekniskt och operativt stöd åt säkerhetstjänsten och polisen.

Genom inhämtning enligt p.1 ovan förser CSE ett flertal kanadensiska myndigheter med underrättelser.

Inhämtningen förutsätter att den ansvarige ministern ger sitt tillstånd till signalspaningen. Spaningen får inte avse personer som befinner i Kanada och inte heller kanadensiska medborgare som befinner sig utomlands. Det kan i praktiken självklart uppstå problem i fråga om en sådan avgränsning. Regeln ska enligt uppgift uppfattas som att det inte får finnas någon avsikt att primärt avlyssna personer i Kanada eller kanadensiska medborgare utomlands.

Ministern ska i samband med tillståndsgivningen förvissa sig om *att* spaningen endast avser utländska mål utanför Kanada, *att* informationen inte kan nås på annat sätt, *att* ändamålet med spaningen står i rimlig proportion till ingreppet samt *att* tillfredsställande åtgärder vidtas för att skydda kanadensiska medborgare och att privat kommunikation får användas endast om det framstår som nödvändigt i förhållande till utrikes förhållanden, försvar eller säkerhet. Ministern kan förena tillståndet med de villkor som han eller hon finner nödvändiga för att skydda kanadensiska medborgares integritet.

Signalspaningen har ingen teknisk begränsning i den meningen att såväl spaning i eter som i tråd är tillåten.

Av tillståndet ska framgå under vilken tid tillståndet gäller. Tillståndet kan därefter förnyas. Ett tillstånd eller en förnyelse av ett sådant tillstånd får inte sträcka sig längre än ett år.

CSE:s stöd åt säkerhetstjänsten och polisen

Canadian Security Intelligence Service (CSIS) är Kanadas säkerhetstjänst. Myndigheten lyder under Public Safety Department, ett av ministerierna i den kanadensiska regeringsadministrationen. CSIS verksamhet är reglerad i Canadian Security Intelligence Service Act (C-23) från år 1984.

CSIS är ingen polismyndighet och saknar därmed polisära, exekutiva befogenheter. De kan däremot använda olika former av teknisk avlyssning som ett led i sin underrättelseinhämtning, t.ex. signalspaning. Begreppet signalspaning används emellertid inte i den lagstiftning som reglerar avlyssningen. Befogenheterna är tämligen generellt angivna och innebär att CSIS kan – i den mån det bedöms strikt nödvändigt – inhämta, analysera och bevara information och underrättelser avseende aktiviteter som på rimlig grund kan antas utgöra hot mot Kanadas säkerhet. Inhämtningen är inte teknikberoende utan kan avse vilken typ av kommunikation som helst (to intercept any communication).

CSIS uppdrag är huvudsakligen att rapportera och ge råd till den kanadensiska regeringen. Myndigheten har också möjlighet att överlämna information till polisen, vilket sker i olika utsträckning beroende på respektive ärendes karaktär. Public Safety Department kan därtill beordra CSIS att bistå polisen i ett ärende, vilket emellertid förekommer endast i undantagsfall.

För att kunna inhämta information genom att avlyssna telekommunikationer krävs tillstånd av en federal domstol. CSIS måste därtill innan ett sådant tillstånd begärs få ett medgivande från den ansvarige ministern. Ansökan till domstolen ska vara skriftlig och ska innehålla skälen för begäran, en beskrivning av vilka andra åtgärder som har vidtagits i ärendet och varför dessa inte varit tillräckliga, vilken typ av kommunikation som ska avlyssnas och vilken person (om detta är känt) som kommer att bli föremål för avlyssning.

Domstolen får som huvudregel inte bevilja tillstånd för längre tid än 60 dagar.

Om domstolen beviljar CSIS tillstånd till avlyssning kan CSIS därefter vända sig till CSE, som enligt sitt uppdrag (se ovan ang. CSE:s uppdrag p.3) ska ge CSIS tekniskt och operativt stöd. CSE är i fråga om sådan avlyssning begränsad av den lagstiftning som reglerar CSIS verksamhet.

CSE kan på samma sätt biträda den federala polisen, Royal Canadian Mounted Police (RCMP), även det en myndighet som

lyder under Public Safety Department. På samma sätt som gäller för CSIS krävs att RCMP har ett tillstånd från domstol och CSE biträder med de begränsningar som följer av den lagstiftning som reglerar RCMP:s verksamhet.

Det finns i Kanada ett regelverk, the Evidence Act, som ger myndigheterna en möjlighet att efter ett särskilt domstolsförfarande använda underrättelsematerial som bevisning i domstol eller att förhindra en sådan användning. Domstolsförfarandet syftar till att öppna möjligheten att använda underrättelsematerial i en rättegång samtidigt som information som inte bör offentliggöras kan behållas hemlig.

Kontrollorgan

Det finns fyra olika kontrollorgan av betydelse i detta sammanhang: the Inspector General, the Security Intelligence Review Committee (SIRC), the Commission for Public Complaints Against the RCMP (CPC) och The Commissioner of the Communications Security Establishment.

The Inspector General biträds av ett sekretariat vid Public Safety Department och rapporterar till biträdande ministern vid departementet. The Inspector General ska för departementets räkning granska CSIS inriktning, interna regelverk och arbetsmetoder samt påtala eventuella brister. Rapporterna är inte offentliga.

SIRC är en kommitté som består av minst två och högst fyra ledamöter utsedda av regeringen. Kommittén biträds av ett sekretariat och utgör en större organisation än the Inspector General. Kommittén har bl.a. i uppgift att studera de rapporter som the General Inspector producerar och att granska regelverk m.m. inom CSIS. Därtill har SIRC i uppdrag att utreda klagomål från enskilda som riktas mot CSIS. SIRC ska årligen överlämna en rapport till den ansvarige ministern, en rapport som ministern i sin tur ska presentera för parlamentet.

CPC undersöker klagomål från enskilda mot RCMP, men har inte samma breda insyn och mandat som SIRC.

The Commissioner of the Communications Security Establishment är ett kontrollorgan med uppgift att kontrollera CSE:s verksamhet. Uppdraget är personligt och den person som utses av regeringen till Commissioner är i allmänhet en hög domare. The Commissioner biträds av ett sekretariat. Kontrollen består i huvudsak av granskningar i efterhand på eget initiativ. The Commissioner har därtill en skyldighet att behandla klagomål från enskilda, vilket

emellertid förekommer i en tämligen ringa utsträckning. Regeringen ska informeras om the Commissioners iakttagelser genom en årlig rapport, en rapport som den ansvarige ministern i sin tur är skyldig att presentera för parlamentet.

I de fall CSE biträder CSIS har även SIRC möjlighet att kontrollera den del av CSE:s verksamhet som är relevant.

6.2.3 Nederländerna

I Nederländerna regleras den civila underrättelse- och säkerhetstjänstens (AIVD) och den militära underrättelse- och säkerhetstjänstens (MIVD) möjligheter att övervaka och avlyssna telekommunikationer i en lag från 2002 (Intelligence and Security Services Act 2002). Den fortsatta redogörelsen kring lagstiftningen tar sikte på enbart AIVD:s befogenheter.

Befogenheten att övervaka telekommunikationer är uppdelad på tre olika bestämmelser (artiklarna 25–27).

Enligt artikel 25 har AIVD rätt att med tekniska hjälpmedel övervaka varje form av telekommunikation eller dataöverföring oavsett var trafiken förekommer (enligt en officiell översättning till engelska: to tap, receive, record and monitor in a directed way any form of conversation, telecommunication or data transfer by means of an automated work, irrespective of where it takes place). Tillstånd till övervakningen lämnas av den ansvarige ministern på begäran av chefen för AIVD. För att tillstånd ska beviljas måste AIVD redogöra för hur övervakningen ska gå till, ange en teleadress (i den mån det är möjligt), identiteten på den person eller den organisation som övervakningen ska avse och skälen för åtgärden. I den mån teleadressen inte är känd vid tiden för ansökan ska tillståndet villkoras på det sättet att övervakningen inte får påbörjas förrän adressen blivit känd. AIVD får använda tekniska hjälpmedel i syfte att identifiera adressen. För det fall identiteten på den person eller organisation som ska övervakas inte är känd vid tiden för ansökan ska tillstånd beviljas endast under den förutsättningen att ansökan kompletteras i det avseendet så snart som möjligt.

AIVD har vidare enligt artikel 26 befogenheten att med tekniska hjälpmedel ta emot och spela in telekommunikation i etern som har sitt ursprung i andra länder eller som är avsedd för andra länder (to receive and record non-cable-bound telecommunication originating or intended for other countries). Sådan övervakning får bedrivas i syfte att följa trafiken och för det syftet behövs inte något tillstånd. Så snart

AIVD har identifierat en avsändare (en person eller organisation) till en specifik telekommunikation och myndigheten önskar fortsätta övervakningen krävs tillstånd på samma sätt som beskrivits ovan.

AIVD har slutligen enligt artikel 27 befogenheten att med tekniska hjälpmedel ta emot och spela in telekommunikationer i etern även i andra fall (to receive and record non-specific non-cabled-bound telecommunication). För att bedriva sådan övervakning behövs inte något tillstånd. AIVD får emellertid inte söka i eller på annat sätt bearbeta den information som inhämtas utan tillstånd från den ansvarige ministern. AIVD kan således utan tillstånd inhämta och lagra informationen, men behöver ett tillstånd för att söka i och bearbeta materialet. I tillståndet anges rätten för AIVD att i syfte att finna kommunikation som är relevant för myndigheten använda identiteten på en person eller organisation, en teleadress eller ett sökbegrepp.

Polisens egna befogenheter regleras i the Dutch Code of Criminal Procedure. Befogenheterna synes i allt väsentligt motsvara sedvanlig hemlig teleavlyssning inom ramen för en förundersökning.

Övervakningen utförs i huvudsak av myndigheterna själva. I Nederländerna finns en organisation, NSO, som biträder med övervakning i etern, dvs. signalspaning i traditionell mening. Organisationen ingår som en del av MIVD, men utför uppdrag även för AIVD och polisen.'

AIVD:s och MIVD:s verksamhet står under kontroll av en kommission, Commissie van toetzicht betreffende de inlichtingenen veiligheidsdiensten. Kommissionen består av tre ledamöter som utses av regeringen. Ledamöterna har rätt till full insyn i myndigheternas verksamhet och ska kontrollera om verksamheten står i överensstämmelse med lagen. Kommissionen rapporterar sina iakttagelser till regeringen.

AIVD kan överlämna information till polisen, men avgör själv om det ska ske och hur informationen får användas. Eventuell sekretess hos AIVD gäller också för polisen. Om AIVD skulle ha tillgång till information av betydelse för en brottsutredning finns en möjlighet att en tjänsteman vid AIVD hörs som vittne inför en domare i en särskilt utpekad allmän domstol. Efter förhöret är det emellertid AIVD som avgör om vittnesutsagan helt eller delvis kan offentliggöras i en rättegång.

Polisen har i sin tur en skyldighet att överlämna information till AIVD för det fall informationen har betydelse för AIVD:s verksamhet. Materialet kan emellertid endast användas av AIVD med de begränsningar som polisen bestämmer.

6.2.4 Tyskland

Inledning

I likhet med i Kanada görs inte heller i tysk rätt någon skillnad mellan signalspaning och hemlig teleavlyssning. Begreppen är okända i tysk rätt och signalspaning och hemlig teleavlyssning, såsom vi uppfattar begreppen i Sverige, är en och samma sak. I tysk lagstiftning används i stället begreppet telekommunikationsövervakning. Det framgår i lagtexterna att övervakningen sker i hemlighet (”ohne Wissen der Betroffenen”).

Telekommunikationsövervakningen kan omfatta trafik som går både i eter och i tråd och den tyska lagstiftningen gör ingen skillnad mellan dessa båda fall. Eterspaning och trådspaning regleras i ett och samma regelsystem och utan att det finns särskilda regler för de båda olika fallen. Övervakningen kan avse såväl avlyssning av telefonsamtal och radiotrafik som uppfångande av andra former av trafik, t.ex. e-post och telefax. Övervakningen kan avse såväl innehållet i meddelandena som övriga trafikuppgifter.

Telekommunikationsövervakning får i Tyskland utföras av såväl underrättelse- och säkerhetstjänster som polisen. Både sådana myndigheter på federal nivå och på delstatsnivå har rätt att använda telekommunikationsövervakning. Var och en av dessa myndigheter har också sina egna tekniska resurser för att genomföra avlyssning och annan övervakning av telekommunikationerna, men det förekommer också att myndigheterna bistår varandra.

Polisens befogenheter

På federal nivå finns det olika lagar som ger myndigheterna rätt att använda telekommunikationsövervakning. Polisen ges en sådan rätt enligt den tyska straffprocesslagen (Strafprozessordnung). I lagtexten anges för vilka brott som telekommunikationsövervakning kan användas. Det rör sig om ett mycket stort antal brott, såsom t.ex. högförräderi och andra brott mot rikets säkerhet, urkundsförfalskning, penningförfalskning, sexualbrott, barnpornografi, mord och dråp, vapenbrott, stöld och häleribrott, penningtvätt samt bedrägeribrott. Andra exempel är att skattebrott, tullbrott och brott mot utlänningslagstiftningen under vissa förutsättningar kan ge rätt att använda telekommunikationsövervakning. Därtill finns en möjlighet att få använda sådan övervakning även vid misstanke om andra brott än de som uppräknas i

lagtexten. Förutsättningen är då att det andra brottet i det enskilda fallet framstår som allvarligt (”schwer wiegt”). Om försök till brott är straffbart får övervakningen också omfatta sådana fall under motsvarande förutsättningar.

För att telekommunikationsövervakning ska få användas krävs att det finns en misstänkt person. Övervakningen (t.ex. avlyssningen) får sättas in mot den personen men också mot andra personer som det finns anledning att anta att den misstänkte har kommunikationstrafik till eller mottar sådan trafik från eller vars kommunikationspunkt (t.ex. teleadress) den misstänkte använder på något sätt.

För telekommunikationsövervakning med stöd av straffprocesslagen krävs tillstånd av domstol. Det är bara åklagare som kan ansöka om tillstånd. Tillstånd kan ges för högst tre månader, men kan förlängas med högst tre månader i taget.

Det finns inte något organ som utför efterhandskontroll av den telekommunikationsövervakning som polisen genomför med stöd av straffprocesslagen. Däremot finns det en skyldighet för åklagaren att i efterhand underrätta en person som har utsatts för telekommunikationsövervakning om att så har skett. Underrättelse ska lämnas så snart det kan ske utan fara för utredningen, för den offentliga säkerheten, för liv eller lem eller för möjligheten att vidare använda en civil spanare. Föreligger något av de nämnda förhållandena får underrättelsen skjutas upp eller helt underlåtas. Regleringen innehåller inga tidsfrister. Frågan om vilka personer som ska anses ha varit utsatta för övervakningen har diskuterats i Tyskland. Praxis har varit olika på federal nivå och inom delstaterna. Det har också funnits skillnader i praxis mellan olika delstater. Praxis innebär att underrättelse lämnas allt mer sällan. Underrättelse till andra än den misstänkte själv, t.ex. till en arbetsgivare när den misstänktes telefon på arbetsplatsen utsatts för avlyssning, anses kunna vara integritetskränkande för den misstänkte.

Polisens möjlighet att bedriva telekommunikationsövervakning med stöd av bestämmelser i straffprocesslagen är inte begränsad till enbart inrikes trafik. Även trafik över landets gränser omfattas.

Information som inhämtats genom telekommunikationsövervakning enligt straffprocesslagen får självfallet användas som bevis i en brottmålsrättegång. Sådan information får också överlämnas till de tyska säkerhets- och underrättelsetjänsterna, om informationen kan anses vara av betydelse för den verksamhet som dessa tjänster ansvarar för. Om informationen ingår i en förundersökning, får

informationen överlämnas endast om den för förundersökningen ansvarige åklagaren har medgivit det.

Teleoperatörerna är skyldiga att medverka till att myndigheterna kan bedriva telekommunikationsövervakning enligt straffprocesslagen. Kostnaderna för detta får teleoperatörerna själva stå för.

Övervakning enligt G 10-lagen

Vid sidan av reglerna i straffprocesslagen finns det också regler i den s.k. G 10-lagen (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) som ger myndigheter möjlighet att bedriva telekommunikationsövervakning. Dessa möjligheter är i G 10-lagen uppdelade på två situationer. Den ena avser övervakning i enskilda fall, den andra s.k. strategisk övervakning.

Telekommunikationsövervakning i enskilda fall får enligt G 10-lagen ske vid misstanke om att någon planerar, begår eller har begått vissa i lagen särskilt angivna brott av allvarligare slag. Det rör sig bl.a. om brott mot rikets säkerhet och mot det demokratiska systemet. Övervakning med stöd av dessa bestämmelser får bara ske om det är utsiktslöst att kunna ta reda på omständigheterna kring brottsmisstanken på andra sätt eller om det annars skulle vara väsentligt svårare att få tag i den informationen. Tillstånd till övervakning ges på federal nivå av den minister i förbundsregeringen som är ansvarig för operationen. Tillstånd kan på motsvarande sätt lämnas på delstatsnivå. Endast den tyska federala säkerhetstjänsten (Bundesverfassungsschutz), de olika delstaternas säkerhetstjänster, den tyska federala utrikesunderrättelsetjänsten (Bundesnachrichtendienst) och den militära säkerhetstjänsten (Militärische Abschirmdienst) får bedriva telekommunikationsövervakning med stöd av bestämmelserna i G 10-lagen om övervakning i enskilda fall.

Vid sidan härav finns i G 10-lagen en möjlighet för utrikesunderrättelsetjänsten att bedriva s.k. strategisk telekommunikationsövervakning av internationella telekommunikationer. Förutsättningarna för att få göra det är mycket restriktivt utformade och omfattar bara fall där det föreligger hot om beväpnat angrepp på Tyskland, internationell terrorism med viss anknytning till Tyskland, spridning av krigsvapen i vissa fall, obefogad införsel av bedövningsmedel (droger) i icke ringa mängder till Tyskland och vissa mer omfattande fall av förfalskning av pengar eller penningtvätt. Strategisk övervakning får också användas i särskilda fall om det är nödvändigt för att i tid kunna fast-

ställa fara för liv och hälsa för en person i utlandet och om därigenom tyska intressen i utlandet påverkas i särskilt allvarlig utsträckning. Ett exempel på det kan vara tagandet av tyska medborgare som gisslan i utlandet men även andra personer än tyska medborgare omfattas om faran direkt eller väsentligen påverkar tyska intressen.

Tillstånd till strategisk övervakning ges av den minister i förbundsregeringen som är ansvarig för underrättelseoperationen, men ska också godkännas av dels ett särskilt kontrollutskott i den tyska förbundsdagen (det parlamentariska kontrollrådet), dels av ett av det utskottet särskilt tillsatt kontrollorgan, den s.k. G 10-kommissionen.

Såväl övervakningen i enskilda fall som den strategiska övervakningen omfattas av en kontroll som G 10-kommissionen ska utföra.

En närmare redovisning av såväl det parlamentariska kontrollrådets som G 10-kommissionens uppgifter och sammansättning och förfarandet vid strategisk övervakning finns i SOU 2006:98 s. 68 ff.

Strategisk övervakning ska ske automatiserat med användning av sökbegrepp. Sökbegreppen får inte utformas så att specifika teleadresser i Tyskland träffas. Däremot är det tillåtet att utforma sökbegreppen så att specifika teleadresser i utlandet träffas, om det kan uteslutas att innehavaren av teleadressen eller den som regelmässigt nyttjar den är tysk medborgare.

Information som har inhämtats genom telekommunikationsövervakning i enskilda fall med stöd av G 10-lagen får överlämnas till polisen för att användas för att förhindra eller klara upp vissa allvarligare brott. Också när det gäller information som inhämtats genom strategisk telekommunikationsövervakning får ett sådant överlämnande ske vid vissa allvarligare brott.

Information som inhämtats genom övervakning med stöd av G 10-lagen får användas som bevisning i rättegång. Om i något fall den myndighet som inhämtat informationen genom telekommunikationsövervakning finner att användandet av informationen som bevisning i rättegång skulle kunna avslöja hemlig information rörande t.ex. myndighetens arbetsformer eller förmåga, kan myndighetens chef besluta att informationen inte får användas som bevis i rättegång. Ett sådant beslut (en s.k. spärrförklaring) kan dock ”överklagas” till förvaltningsdomstol såväl av åklagaren som av den som är försvarare för den misstänkte.

Teleoperatörerna är skyldiga till att medverka också till den telekommunikationsövervakning som bedrivs med stöd av G 10-lagen. Kostnaderna för detta får teleoperatörerna själva stå för.

6.3 Slutsatser kring de svenska förhållandena

En slutsats av redovisningen är att det är svårt att utan vidare jämföra svenska myndigheter och den svenska lagstiftningen med motsvarigheter utomlands. Svårigheten gör sig gällande såväl vad gäller myndigheternas uppdrag och ansvarsområden som de befogenheter som följer av lag.

Jag har i avsnitt 1.2.3 redogjort för hur förhållandena i Sverige på ett antal viktiga punkter skiljer sig från förhållandena i de flesta jämförbara länder. Jag har i det avsnittet också redogjort för hur dessa skillnader inverkar på de förslag som jag redovisar i detta betänkande.

7 Överväganden och förslag

7.1 Polisens behov av signalspaning

Bedömning: Det finns ett behov inom polisen att använda signalspaning som en inhämtningsmetod bland flera andra. Behovet skiljer sig emellertid åt mellan Säkerhetspolisen och den övriga polisen.

7.1.1 Inledande synpunkter

Frågan om polisen har behov av signalspaning eller inte är naturligtvis ytterst en fråga om vilken ambitionsnivå som ska gälla i polisens verksamhet. Ju större krav på resultat i den brottsförebyggande och brottsutredande verksamheten, desto större är polisens behov av resurser och effektiva verktyg.

Signalspaning har använts inom polisen sedan 1940–talet. Tekniken har förändrats över tid liksom inriktningen av spaningen. Så har exempelvis spaningen på polisens uppdrag mot den s.k. agentradiotrafiken sedan några år upphört (se avsnitt 3.2), medan annan typ av signalspaning har utvecklats. I Sverige och dess närhet spelar teknikutvecklingen en avgörande betydelse för polisens behov av signalspaning. Den signalspaning som bedrivits hittills har uteslutande rört sig om spaning i etern. I takt med att en allt större del av trafiken sker i tråd har signalspaning i etern efter hand minskat i betydelse. Frågan om spaning i tråd är ny och nyttan av en sådan spaning därmed givetvis svårbedömd.

En redogörelse för polisens behov av signalspaning blir därför tudelad. Såvitt gäller den spaning i etern som bedrivits i flera årtionden handlar det i första hand om en bedömning av vilken förmåga som går förlorad om polisen fortsättningsvis inte ska kunna använda sig av den typen av spaning. När det gäller signalspaning i

tråd rör det sig om en eventuell ny befogenhet och bedömningen måste göras kring en förväntad nytta med den typen av spaning.

Samtidigt skulle en återgång till den tidigare ordningen, dvs. att återskapa en möjlighet för polisen att signalspana i etern, i praktiken innebära en försämrad förmåga för polisen i takt med att den eterburna trafiken minskar till förmån för trådbunden trafik. På samma sätt kan en befogenhet för polisen att signalspana i tråd – en befogenhet som polisen hittills inte haft – inte enbart ses som en ökning av polisens förmåga jämfört med tidigare. En sådan ny befogenhet skulle till en del enbart svara mot den tidigare förmåga polisen hade genom signalspaning i etern.

Det kan tilläggas att inte i något av de länder jag studerat inom ramen för utredningsuppdraget står ländernas säkerhetstjänster och polisorganisationer helt utan möjlighet att erhålla information som inhämtats genom signalspaning.

7.1.2 En inhämtningsmetod bland flera

Som framgått ovan (avsnitt 5) fyller signalspaningen inom polisen sin viktigaste funktion som en inhämtningsmetod bland flera inom den säkerhetsunderrättelseverksamhet som bedrivs vid Säkerhetspolisen. Vid sidan av andra inhämtningsmetoder, t.ex. mänskliga källor och traditionell spaning, ger signalspaningen möjlighet att bedöma hot och upptäcka eventuell brottslig verksamhet.

Signalspaningen har som en isolerad spaningsmetod sällan en avgörande betydelse i enskilda ärenden för vare sig Säkerhetspolisen eller den övriga polisen. Den information som kan framkomma genom signalspaning kan emellertid följas upp och kompletteras med annan typ av spaning eller med åtgärder inom ramen för en förundersökning. Därtill kan tips och uppslag som inkommer till polisen, t.ex. från källor eller samverkande myndigheter utomlands, följas upp genom signalspaning. Med den sammanlagda informationen kan misstankar om att det pågår brottslig verksamhet därefter antingen stärkas eller avfärdas. För det fall misstankarna stärks kan ofta en förundersökning inledas och, om förutsättningarna för det är uppfyllda, straffprocessuella tvångsmedel användas. På samma sätt kan misstankar om eventuell säkerhetshotande verksamhet avfärdas.

Betydelsen av signalspaning som ett komplement till andra spaningsinsatser är i detta avseende stor. Den information som kan

inhämtas genom signalspaning kan inte inhämtas med samma kvalitet på annat sätt.

7.1.3 Behovet av kunskap om utrikes förhållanden

Säkerhetspolisens verksamhet avser till stor del utrikes förhållanden. De brott som myndigheten har att förebygga och uppdaga har ofta sin grund utomlands, t.ex. en hos främmande makt eller en organisation med säte utomlands. För att kunna kartlägga den typen av brottslighet krävs kunskaper om utrikes förhållanden.

Varken Säkerhetspolisen eller den övriga polisen har några befogenheter att bedriva polisverksamhet utanför landets gränser. Kunskapen om utrikes förhållanden måste därmed tillgodoses på annat sätt. Ett sätt är att samverka med myndigheter i andra länder, vilket också förekommer. Ett sådant utbyte har självfallet sina begränsningar dels i fråga om det urval av information som en svensk myndighet kan få tillgång till, dels i fråga om tillförlitligheten i informationen.

Användningen av signalspaning, såvitt gäller den fjärrspaning som Försvarets radioanstalt har bedrivit på uppdrag av polisen, har syftat till att täcka delar av polisens behov av kunskap om utrikes förhållanden. Signalspaningen är ett sätt att på egen begäran – och med svenska myndigheters underrättelsebehov för ögonen – få tillgång till förstahandsinformation om utländska förhållanden av betydelse för polisens uppdrag.

Det råder ingen tvekan om att Säkerhetspolisen och övriga polisen är beroende av kunskap om utrikes förhållanden för att fullgöra sitt uppdrag. Signalspaning framstår som ett viktigt instrument för att tillgodose det behovet. Tillgången till förstahandsinformation och möjligheten att inrikta inhämtningen efter egna behov är viktiga faktorer som talat för att polisen ska ha fortsatt tillgång till signalspaning.

7.1.4 Betydelsen av signalspaning inom underrättelseverksamheten

Signalspaning har inom både Säkerhetspolisen och den övriga polisen framför allt använts som en inhämtningsmetod inom ramen för säkerhetsunderrättelseverksamheten och kriminalunderrättelseverksamheten.

Säkerhetspolisens verksamhet är till sin största del brottsförebyggande. Den brottslighet myndigheten har i uppdrag att motverka och bekämpa sker i det dolda. En väsentlig del av uppdraget är därför att genom underrättelseverksamhet undersöka om någon, t.ex. en främmande makt eller internationell organisation, har avsikten och förmågan att begå brott i syfte att skada Sverige eller svenska intressen. Om så skulle visa sig vara fallet ska hotet identifieras och motåtgärder sättas in.

Signalspaning har visat vara en värdefull inhämtningsmetod i underrättelsearbetet. Genom signalspaning har exempelvis utländska organisationers utbredning och kommunikationsmönster kunnat kartläggas och analyseras. För det fall information från exempelvis signalspaning ger vid handen att organisationen i fråga har intressen riktade mot Sverige kan underrättelseinhämtningen breddas och fördjupas.

7.1.5 Betydelsen av signalspaning inom utredningsverksamheten

Som framgår av avsnitt 4.1.2 är det inte möjligt för Försvarets radioanstalt att bistå polisen med signalspaning inom ramen för en förundersökning.

Som beskrivits ovan är det heller inte inom brottsutredningsverksamheten som signalspaningen har sin stora betydelse. Det finns emellertid situationer där signalspaningen även inom den brottsutredande verksamheten skulle kunna kan utgöra en värdefull metod, framför allt som ett komplement till hemlig teleavlyssning och hemlig teleövervakning. Det kan exempelvis röra sig om situationer där det en känd teleadress saknas. Vidare kan det röra sig om situationer där en hemlig teleavlyssning inte kan verkställas därför att den person som ska avlyssnas befinner sig i ett land där den hemliga teleavlyssningen inte går att verkställa med stöd av det landets myndigheter.

Signalspaning i tråd företer naturligtvis stora likheter med hemlig teleavlyssning, såväl i teknisk mening som med avseende på den information som är möjlig att inhämta. I den mån sådan signalspaning ska kunna användas inom ramen för en förundersökning bör emellertid krävas att de förutsättningar är uppfyllda som gäller för de straffprocessuella tvångsmedlen. En viktig utgångspunkt är att signalspaningen inte ska användas som ett sätt att kringgå de bestämmelser som reglerar polisens verksamhet. En förundersökning syftar till att utreda vem som skäligen kan misstänkas för ett konkret brott och om tillräckliga skäl föreligger för ett åtal mot honom eller henne (23 kap. 2 § rättegångsbalken). Förundersökningen är kringgärdad av en mängd bestämmelser som syftar till att garantera den misstänkte rättssäkerhet och insyn. De tvångsmedel som står polisen till buds regleras i främst rättegångsbalken och polislagen (1984:387). Varje tvångsmedel kringgärdas av särskilda bestämmelser i syfte att garantera en rättssäker användning. Det kan knappast ha varit lagstiftarens avsikt att polisen, utan iakttagande av de rättssäkerhetsgarantier som kringgärdar framför allt de straffprocessuella tvångsmedlen, samlar information på ett sätt som är förenat med en avsevärd integritetskränkning av enskilda individer.

7.1.6 Uppdelning av signalspaningen för olika syften?

Som nämnts ovan (avsnitt 4.1.2) har det numer tydliggjorts att Försvarets radioanstalt inom ramen för försvarsunderrättelseverksamheten inte kan bistå polisen med signalspaning i en förundersökning. Som konstaterats ovan är behovet av signalspaning inom polisen också som störst inom Säkerhetspolisens underrättelseverksamhet. Behovet inom utredningsverksamheten handlar både för Säkerhetspolisens och den övriga polisens del i huvudsak om att komplettera de befintliga hemliga tvångsmedlen, främst hemlig teleavlyssning.

Övervakningen av telekommunikationer inom underrättelseverksamheten respektive utredningsverksamheten har olika syften. Medan polisen i sin underrättelseverksamhet kartlägger förhållanden och uppdagar brottslig verksamhet, driver polisen i utredningsverksamheten en brottsutredning i syfte att klarlägga omständligheterna kring ett konkret brott.

I flera länder jag har studerat finns beträffande avlyssning av telekommunikationer inom de civila säkerhetstjänsterna tämligen

generösa bestämmelser. Befogenheterna är ofta långtgående, men kompletteras samtidigt av kontroll- och insynsmekanismer. De befogenheter som tillkommer de brottsutredande myndigheterna är ofta mer begränsade. De utländska systemen har ofta sin grund i att säkerhetstjänsterna i dessa länder enbart bedriver underrättelseverksamhet, dvs. de saknar polisiära befogenheter. Jag har i avsnitt 6.1 redovisat förhållandena i några andra länder i syfte att belysa de olika myndigheternas ansvarsområden och underrättelseverksamhetens struktur.

Det kan möjligen te sig naturligt att skapa en lagstiftning kring signalspaning som enbart tar sikte på inhämtning inom ramen för Säkerhetspolisens underrättelseverksamhet, eller att i vart fall utforma särskilda regler för de båda verksamhetsgrenarna. En sådan lösning skulle också överensstämma med den lösning som statsmakterna valt när det gäller polisens möjlighet att inrikta försvarsunderrättelseverksamheten.

I Sverige måste emellertid hänsyn tas till att Säkerhetspolisen både utgör landets säkerhetstjänst och samtidigt utgör en polismyndighet som bedriver egna brottsutredningar inom sitt ansvarsområde. Med den polisiära delen av Säkerhetspolisens uppdrag följer de skyldigheter som ankommer på varje polismyndighet och på de polismän som är anställda vid en sådan myndighet. Som exempel kan nämnas varje polismans skyldighet enligt 9 § polislagen (1984:387) att rapportera brott som kommer till hans eller hennes kännedom och myndighetens skyldighet att inleda förundersökning för det fall det finns anledning att anta att ett brott under allmänt åtal har förövats (23 kap. 1 och 3 §§ rättegångsbalken). Säkerhetspolisen har alltså, till skillnad från de flesta säkerhetstjänsterna i andra länder, en skyldighet att agera polisiärt på grund av vad som kommer till myndighetens kännedom. Denna skyldighet är naturligtvis inte beroende av i vilken organisatorisk del av verksamheten som informationen kommer till myndighetens kännedom.

Säkerhetspolisens tudelade uppdrag har självfallet praktiska konsekvenser för verksamheten. Såväl organisationer som enskilda individer kan vara föremål för Säkerhetspolisens intresse såväl inom underrättelseverksamheten som inom utredningsverksamheten. En person som är misstänkt för brott i en pågående förundersökning kan ju samtidigt bedömas värdefull att följa från ett underrättelseperspektiv med syftet att förhindra att den misstänkte medverkar till nya brott. Ett förbud mot signalspaning avseende personer och händelser som förekommer inom ramen för en förundersökning får

därmed en direkt återverkning på möjligheten att använda signalspaning mot samma personer eller företeelser i underrättelseverksamheten. Att mot bakgrund av vad som kommer till myndighetens kännedom inom ramen för underrättelseverksamheten inleda en förundersökning, blir därmed från denna utgångspunkt kontraproduktivt. Möjligheten att bedriva underrättelseverksamhet med stöd av signalspaning minskar på grund av den brottsutredningen. Samtidigt är beslutet att inleda en förundersökning en skyldighet som följer av lag.

Att strikt dela upp Säkerhetspolisens verksamhet i en underrättelseverksamhet respektive en utredningsverksamhet låter sig därför svårligen göras inom ramen för ett lagstiftningsarbete, även om myndigheten naturligtvis rent praktiskt kan dela upp sin verksamhet i olika verksamhetsgrenar.

Av vad jag nu anfört (jfr. vad jag framhållit under avsnitt 1.2.2) följer att Säkerhetspolisen har behov av underrättelser om utländska förhållanden såväl utan samband med att en förundersökning pågår som under en förundersökning. När det gäller Säkerhetspolisens uppgift att bekämpa hot mot svensk nationell säkerhet eller internationell säkerhet måste lagstiftningen därför utformas på ett sådant sätt att ett inledande av förundersökning inte hindrar att signalspaning kan användas i det arbetet. Det vore förödande för Sveriges förmåga att möta ett allvarligt säkerhetshot, om möjligheten att med hjälp av signalspaning klarlägga t.ex. hotets mål, tidpunkt för genomförande och tilltänkta gärningsmän stoppas bara därför att åklagare och polis på grund av lag är tvingade att inleda förundersökning om brottet.

En annan sak är att det material polisen erhåller från Försvarets radioanstalt ofta måste skyddas från insyn, vilket begränsar möjligheten att använda sådant material inom ramen för en förundersökning. Den frågan återkommer jag till senare (se avsnitt 7.12).

7.1.7 Spaning i eter eller tråd?

Vad gäller teknikutvecklingen kan generellt sägas att polisens verktyg måste vara anpassade till förhållandena i omvärlden. Som nämnts tidigare har kommunikationstekniken utvecklats snabbt under senare år. Uppbyggnaden av det globala nätet har ändrat förutsättningarna för enskilda personer att kommunicera med varandra. En rimlig

utgångspunkt är att polisens verktyg måste moderniseras i samma takt, i vart fall om avsikten är att bevara polisens förmåga.

Mot den bakgrunden kan slutsatsen dras att om det inom polisen kan anses föreligga ett behov av signalspaning kommer spaningen i tråd att alltmer öka i betydelse, medan betydelsen av spaning i etern i motsvarande utsträckning kan förväntas minska. Att återskapa polisens möjlighet till spaning i etern, dvs. i princip en återgång till de förhållanden som rådde mot bakgrund av att etern ansetts fri att avlyssna, innebär därmed inte att polisen återfår den förmåga man har haft under tidigare år. En sådan lösning innebär därmed i praktiken en minskad förmåga jämfört med tidigare.

En bibehållen förmåga för polisens del måste mot denna bakgrund därmed innefatta en befogenhet att signalspana i tråd. Med en sådan lösning kommer emellertid polisens förmåga inte bara att bibehållas utan även öka. En sådan befogenhet måste i så fall kringgärdas med avsevärda rättssäkerhetsgarantier.

I de länder jag har studerat närmare sker spaning i såväl eter som i tråd, låt vara att regleringarna skiljer sig åt länderna emellan. I exempelvis Kanada gäller samma förutsättningar för spaningen i etern som i tråd, medan det i Nederländerna görs viss skillnad (se avsnitt 6.2).

7.1.8 Förhållandet till försvarsunderrättelseverksamheten

Jag ska enligt mina direktiv utforma mina förslag på ett sådant sätt att förhållandet mellan signalspaning i försvarsunderrättelseverksamhet och motsvarande underrättelseinhämtning i polisiär verksamhet tydliggörs.

Försvarets radioanstalts biträde till polisen med signalspaning har hittills vilat på två olika grunder. Tidigare hade Försvarets radioanstalt bl.a. i uppdrag att bedriva signalspaning på uppdrag av regeringen, Försvarsmakten och övriga uppdragsgivare. Polisen gavs såsom övrig uppdragsgivare en sådan möjlighet att få biträde. Sedan den 1 januari 2008 har polisen i stället haft möjlighet att inrikta Försvarets radioanstalts verksamhet enbart inom ramen för försvarsunderrättelseverksamheten.

I samband med lagstiftningsarbetet inför den ovan nämnda förändringen diskuterades gränsdragningen mellan polisens verksamhet och försvarsunderrättelseverksamheten. Ett antal remissinstanser uttryckte bl.a. farhågor om att gränsdragningen mellan polisens verksamhet och

den verksamhet som bedrivs inom försvarsunderrättelseverksamheten skulle bli otydlig. Synpunkterna föranledde statsmakterna bl.a. att klart uttala att den verksamhet som bedrivs inom försvarsunderrättelseverksamheten inte är brottsbekämpande (se prop. 2006/07:63 s. 31 ff och 36 ff).

Det ligger inte i mitt uppdrag att formulera innehållet i försvarsunderrättelseverksamheten. För att i möjligaste mån åstadkomma en tydlig avgränsning bör polisens signalspaning i stället regleras skild från den signalspaning som bedrivs i försvarsunderrättelseverksamheten. Signalspaning för polisens räkning bör således ske utan koppling till försvarsunderrättelseverksamheten. En sådan lösning följer i praktiken redan av den överenskommelse mellan partierna i regeringen kring signalspaning inom försvarsunderrättelseverksamheten, av vilken framgår att signalspaning i den verksamheten endast ska få bedrivas av Försvarets radioanstalt på beställning av regeringen, Regeringskansliet och Försvarsmakten. Överenskommelsen har numer kommit uttryck i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201).

7.1.9 Särskilt om närspaningen

Även om närspaningen, dvs. spaning mot signaler där avsändaren och mottagaren finns i Sverige, inte varit omfattande under senare år kan den ha avgörande betydelse för polisen när den väl används.

De situationer där metoden kommer till nytta berör främst den vanliga polisens verksamhet, t.ex. att avlyssna radiotrafik mellan medlemmarna i en grupp som står i begrepp att utföra ett värdetransportrån.

Av mina direktiv framgår att jag ska utreda behovet av underrättelser om utländska förhållanden. Även om det enligt direktiven står mig fritt att ta upp och lämna förslag i närliggande frågor, har jag valt att begränsa mina förslag till att avse fjärrspaning, dvs. signalspaning där antingen avsändaren eller mottagaren av ett meddelande (eller båda) befinner sig utomlands.

Närspaning kan utföras på olika sätt och kan användas i olika syften. Gemensamt för olika former av närspaning är emellertid att de utgör teknikbundna spaningsmetoder inom polisen. Polismetodutredningen (Ju 2008:01) har bl.a. i uppdrag att överväga i vad mån den användning av tekniska metoder som i dag förekommer hos de brottsbekämpande myndigheterna bör regleras i

lag (Dir. 2007:185). Polismetodutredningen bedriver sitt utredningsarbete parallellt med mitt. Efter samråd med Polismetodutredningen har den överenskommelsen träffats att frågan om polisens närspaning utreds inom ramen för Polismetodutredningens uppdrag.

7.2 Avvägningen mot integritetsintresset

Bedömning: Om signalspaning i etern, som hittills ansetts helt fri att bedriva, fortsättningsvis ska vara tillåten bör metoden begränsas i lag och kringgärdas av skyddsregler för enskilda.

Om möjlighet ska finnas att även bedriva signalspaning i tråd måste den metoden bli föremål för avsevärda begränsningar i lag och kringgärdas av ett omfattande skydd för enskildas personliga integritet. Metoden kan annars inte motiveras.

Att brottsbekämpande myndigheter i sin verksamhet är beroende av att använda integritetskränkande metoder är en självklarhet. Lika självklart är att användningen av sådana metoder måste begränsas och ställas mot andra intressen, främst skyddet av människors personliga integritet.

Avvägningen är inte lätt och kan heller aldrig anses fastslagen en gång för alla. Tyngden i argument som rör polisens effektivitet skiftar med förhållandena i omvärlden. Ju allvarligare hot mot samhället och enskilda individer, desto större torde förståelsen för integritetskänsliga arbetsmetoder vara.

En grundläggande utgångspunkt är att de brottsbekämpande myndigheterna aldrig kan fungera effektivt utan medborgarnas förtroende. Förtroendet är resultatet av att den förväntan medborgarna har på myndigheterna står i en rimlig överensstämmelse med det arbete som utförs och det resultat som redovisas.

En viktig utgångspunkt är att polisens befogenheter aldrig får vara så omfattande att en vanlig, laglydig medborgare känner en oro för att samhällets institutioner på ett omotiverat sätt övervakar och registrerar enskilda individer. En sådan oro leder till en misstro mot myndigheterna.

Polisens befogenheter får å andra sidan inte vara så begränsade att samhället inte kan tillgodose rimliga krav från medborgarnas sida på trygghet. Även den situationen leder till en misstro mot de brottsbekämpande myndigheterna.

En ytterligare utgångspunkt är att ju mer integritetskränkande metoder som används, desto större måste precisionen i användningen av metoden vara. Mindre ingripande åtgärder från polisens sida, t.ex. att bilförare då och då får finna sig i att utsättas för en nykterhetskontroll, kan tolereras även om urvalet av de personer som utsätts för åtgärden är rent slumpmässigt och därmed oskyldiga drabbas. Annorlunda förhåller det sig med polisiära metoder som innebär ett avsevärt ingrepp i integriteten. Att utsättas för sådana ingrepp utan att det finns en stark misstanke om ett allvarligt brott eller att det föreligger ett allvarligt säkerhetshot ska naturligtvis inte tolereras.

Införandet av nya polisiära befogenheter – liksom motiveringen att behålla redan befintliga metoder – måste således vägas mot allmänhetens oro för obefogade ingrepp i den personliga integriteten, polisens möjligheter att skydda samhällets institutioner och medborgarna mot brott samt risken för att medborgare utsätts för åtgärder som inte står i rimlig proportion till graden av misstanke eller brottets svårighet.

Vad gäller signalspaning för polisens behov kan först beaktas att metoden har använts sedan andra världskriget, låt vara att inriktning och teknik har skiftat genom åren. Metoden har, utom såvitt gäller närspaningen, syftat till att skapa kunskap om utrikes förhållanden och har därmed inte varit en metod som har använts generellt inom polisen. Metoden har i stället enbart använts inom delar av Säkerhetspolisens verksamhet och i en begränsad utsträckning även inom Rikskriminalpolisens verksamhet.

Det smala användningsområdet och inriktningen på utländska förhållanden har säkerligen bidragit till att signalspaningen, såvitt gäller den spaning i etern som det hittills har rört sig om, inte på något tydligt sätt har ifrågasatts från ett integritetsperspektiv. Verksamheten har därtill vilat på den grunden att etern har ansetts fri att avlyssna, även för polisen. Någon särskild befogenhet har inte ansetts behövas och därmed har metoden inte heller kringgärdats med regler om tillstånd och kontroll. Till detta bör läggas att resultatet av signalspaningen har presenterats i form av underrättelserapporter som inte har kunnat användas som bevisning i domstol.

Vad som nu aktualiserar en tydligare avvägning mellan nyttan av signalspaning och skyddet av enskildas integritet är dels den tekniska utvecklingen med utbyggnaden av det globala nätet, dels frågan om att tillåta signalspaning i tråd. Med det globala nätet kan den enskilde användaren av ett kommunikationsmedel inte längre

själv påverka på vilket sätt meddelandet når mottagaren och vilka vägar det tar. Ett och samma meddelande – oavsett om det rör sig om ett telefonsamtal, ett mobiltelefonsamtal, ett e-postmeddelande eller annan telekommunikation – kan vara såväl luftburet som kabelbundet. I vårt närområde är redan i dag trådburen trafik den allt dominerande och väntas framöver dominera än mer.

Möjligheten att signalspana i trådburen trafik skulle därmed redan i dag ge polisen möjlighet att ta del av en mycket stor del av den kommunikation som korsar landets gränser. Avlyssning av trådburen trafik har historiskt ansetts vara avsevärt mer integritetskränkande än att avlyssna luftburen trafik. Signalspaning som metod betraktad skulle därmed framstå som en väsentligt mer integritetskränkande spaningsmetod än vad fallet varit hittills.

Det är min uppfattning att framför allt Säkerhetspolisens behov av kunskaper om utrikes förhållanden måste tillgodoses i någon form. Signalspaning framstår som den enda metoden som både tillgodoser det behovet och som samtidigt svenska myndigheter har en rådighet över. Att enbart återskapa den möjlighet till signalspaning i etern som polisen använt i årtionden synes inte vara meningsfullt. En alltför ringa del av trafiken är eterburen för att tillgodose polisens behov. För att signalspaning ska vara en meningsfull inhämtningsmetod krävs därför att även trådbunden trafik omfattas.

Som nämnts skulle en befogenhet för polisen att spana mot trådburen trafik innebära en möjlighet att spana mot en mycket stor mängd enskilda meddelanden. I enlighet med utgångspunkterna ovan kräver en sådan befogenhet en avsevärd precision i användningen. Som jag nämnt tidigare är medborgarnas förtroende för polisen och dess metoder avgörande. Risken att oskyldiga drabbas eller att systemet kan komma att missbrukas kan medföra att förtroendet minskar. I förlängningen saknar polisen under sådana förutsättningar möjlighet att fullgöra sitt uppdrag. En befogenhet att signalspana i tråd bör således inte införas utan ett omfattande regelverk till skydd för enskilda individers personliga integritet. Ett sådant system måste enligt min mening utformas så att polisen inte får tillgång till all trafik som går i den signalbärare som polisen med stöd av domstols tillstånd skulle få avlyssna. I stället bör åtgärder vidtas för att begränsa polisens tillgång till sådana uppgifter som rör det som utgjort skäl för att domstolen meddelat tillståndet. Vidare måste införas ett system för insyn och kontroll som motverkar varje form av missbruk. I annat fall kan metoden enligt min mening inte motiveras.

Ett sätt att begränsa polisens tillgång till den stora mängd information som är trådbunden är att inte låta polisen själv genomföra sådan spaning. Genom att Försvarets radioanstalt i stället utför spaningen, vilket ju också har varit fallet hittills, kan ett system skapas som förhindrar att polisen får tillgång till annan information än sådan som omfattas av domstols tillstånd. Det blir då endast denna information som redovisas till polisen av Försvarets radioanstalt. Jag återkommer till den frågan i avsnitt 7.8.

7.3 Allmänna förutsättningar för polisens signalspaning

Bedömning: Polisen ska som huvudregel inte få bedriva eller låta bedriva signalspaning.

Jag har redan konstaterat att signalspaning typiskt sett är en spaningsmetod som är av mycket integritetskränkande karaktär. Det bör därför inte komma i fråga att metoden ges en mer generell användning inom polisen. Så har heller aldrig varit fallet historiskt. Däremot har det hittills ansetts att signalspaning i etern kunnat bedrivas fritt. Några begränsningar för polisen att bedriva sådan spaning har således inte gällt.

Enligt min mening är signalspaning, även om den avser enbart etern, en så pass integritetskränkande åtgärd, att möjligheten för polisen att fritt använda den bör avskaffas. I stället bör det införas ett regelsystem som avväger polisen berättigade intresse av att kunna bedriva sådan spaning för att motverka brottslighet eller hot mot rikets säkerhet mot de integritetshänsyn som måste tas. Med hänsyn till styrkan av det intrång i integriteten som signalspaning innebär, är det min uppfattning att det endast undantagsvis finns skäl att låta intresset av effektivitet i arbetet med att avslöja, utreda eller hindra brott väga tyngre än intresset av att skydda den personliga integriteten. Huvudregeln måste därför enligt min mening vara att polisen inte ska få bedriva eller låta bedriva signalspaning. Undantag från denna huvudregel bör göras endast i sådana fall då det gäller allvarlig brottslighet eller betydande nationella eller internationella säkerhetsintressen. Inte heller i dessa fall bör det emellertid alltid vara tillåtet med signalspaning. Betydande begränsningar bör göras även i sådana fall. Begränsningarna bör utformas så att den

vanliga polisen endast i sällsynt förekommande fall ska få tillgripa signalspaning. När det gäller den svenska säkerhetstjänsten (Säkerhetspolisen) bör det – i likhet med vad som gäller i de främmande stater vars system jag studerat – finnas något vidare möjligheter till undantag från huvudregeln. Dessa undantag bör vara kopplade till väsentliga nationella eller internationella säkerhetsintressen.

Eftersom spaning i etern sker mot kommunikationer som kan avlyssnas eller uppfångas av ett stort antal aktörer och den som låter befordra kommunikation på det sättet måste räkna med att den kan komma att avlyssnas eller uppfångas, framstår integritetsintresset som något svagare än vad gäller kommunikation som befordras i tråd. Detta gäller även om det många gånger för avsändare och mottagare är okänt eller slumpmässigt huruvida deras kommunikation går helt eller delvis i kabel eller eter. Min uppfattning är därför att det bör gälla strängare förutsättningar för signalspaning i tråd än för sådan spaning i etern.

I det följande ska jag gå närmare in på i vilka fall som undantag från huvudregeln framstår som motiverade. Såvitt gäller signalspaning i tråd är det min uppfattning att stor restriktivitet bör iakttas när det gäller att göra sådana undantag. Vid utformningen av undantagen måste också särskilt beaktas att dessa undantag inte får möjliggöra ett kringgående av de lagregler som begränsar polisens möjligheter att använda hemlig teleavlyssning.

Mitt förslag är således sammanfattningsvis att huvudregeln för svensk del – till skillnad från vad som är fallet i flera av de länder vars system jag studerat – ska vara att polisen inte ska få bedriva eller låta bedriva signalspaning avseende utländska förhållanden.

Vad som nu anförts gäller signalspaning avseende utrikes förhållanden. När det gäller den s.k. närspaningen hänvisas till vad som anförts i avsnitt 7.1.9.

7.4 Begränsningar i fråga om signalspaning i etern

Förslag: Signalspaning i etern ska få användas endast i syfte att avslöja och utreda eller förhindra brott för vilket är föreskrivet fängelse två år eller däröver. Inom Säkerhetspolisens ansvarsområde ska signalspaning få användas också i andra fall då allvarliga hot mot nationell eller internationell säkerhet motiverar det.

Signalspaning får dock bara användas om syftet med spaningen väger klart tyngre än det integritetsintrång som spaningen kan medföra och om det syftet inte kan tillgodoses på ett mindre ingripande sätt.

Signalspaningen får inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige.

7.4.1 Det generella tillämpningsområdet

Som jag redan anfört bör signalspaning i etern inte längre få ske fritt. Vad gäller brottsbekämpning bör en avgränsning ske så att endast brott av en viss svårighetsgrad träffas. Det bör vara fråga om brott för vilka det föreskrivs fängelsestraff. Men inte ens alla sådana brott är av den karaktären att det vid en avvägning mot integritetsintresset framstår som motiverat att tillåta polisen att få rätt till signalspaning i etern, även om det står envar enskild (t.ex. massmedia och allmänhet) fritt att bedriva sådan spaning. Det finns en del brott för vilka det i straffskalan finns fängelse i sex månader, men där det normala straffet i praxis inte är fängelse utan i stället böter. I sådana fall framstår det inte som motiverat vid intresseavvägningen att tillåta att polisen ska få tillgång till signalspaning ens i etern.

Inte ens i de fall där fängelse utgör en normalpåföljd framstår signalspaning i etern alltid som motiverad med beaktande av de integritetsintrång som kan bli följden av sådan spaning. En rimlig nivå är därför att begränsa användningen av signalspaning i etern för polisens del till att avse brott för vilket är föreskrivet fängelse i två år eller däröver, dvs. maximistraffet för brottet får inte understiga fängelse i två år. Inte ens i sådana fall kan det dock alltid vara rimligt att signalspaning i etern får ske. I många fall måste brottet, även om maximistraffet för brottet är så högt som nyss anförts, anses vara sådant att det inte framstår som rimligt att använda signalspaning i etern med hänsyn till det integritetsintrång som sådan spaning kan medföra. En avvägning måste därför ske i det enskilda fallet mellan intresset av att kunna bekämpa brottsligheten i fråga och integritetsintrånget. Till den frågan återkommer jag i avsnitt 7.4.3. Vad jag nu har anfört innebär en avsevärd begränsning i användningen av signalspaning i etern jämfört med tidigare mot den bakgrunden att sådan signalspaning i etern hittills har kunnat bedrivas helt fritt.

Signalspaning i etern ska enligt min mening få bedrivas såväl i underrättelsesyfte som inom ramen för en brottsutredning. Som redogjorts för tidigare har signalspaning historiskt haft sin stora betydelse som en inhämtningsmetod inom underrättelseverksamheten. Behov finns emellertid även av signalspaning i etern inom ramen för en brottsutredning. Som jag nämnt tidigare är en uppdelning av spaningen för dessa olika syften varken ändamålsenlig eller praktiskt tillämpbar. Användningen av signalspaning inom ramen för en brottsutredning kan emellertid komma att begränsas avsevärt med hänsyn till att materialet som inhämtas genom spaningen som regel inte kan offentliggöras. Jag återkommer till den frågan (se avsnitt 7.12).

7.4.2 Brott som rör rikets säkerhet m.m.

Generellt bör således gälla att polisen inte får använda signalspaning i etern annat än vid brott för vilka föreskrivs fängelse två år eller däröver. Den förutsättningen gäller för hela polisen, dvs. såväl Säkerhetspolisen som den övriga polisen.

För Säkerhetspolisens del finns skäl att även överväga delvis andra förutsättningar för användningen av signalspaning i etern. Som framgått i beskrivningen av Säkerhetspolisens användning av signalspaning (avsnitt 5.2) har en avsevärd del av Säkerhetspolisens verksamhet en tydlig koppling till utrikes förhållanden. Verksamheten i den delen består till stor del av att kartlägga förhållanden i Sverige och utomlands och att uppdaga planer på brottlig verksamhet i syfte att avstyra dessa. Syftet med verksamheten är således att något brott över huvud taget inte ska komma till stånd. Det är därmed inte möjligt att inom Säkerhetspolisens ansvarsområde avgränsa möjligheterna att använda signalspaning till konkreta brott med angivande av särskilda straffskalor, i vart fall inte om spaningen ska täcka det behov av information som finns inom Säkerhetspolisen.

Samtidigt som det inte är möjligt att avgränsa Säkerhetspolisens användning av signalspaning på samma sätt som för den övriga polisen kan det inte ens när det gäller spaning i etern komma i fråga att Säkerhetspolisen fritt skulle få använda signalspaning. Användningen måste begränsas till sådana verksamhetsområden som framstår som särskilt angelägna från samhällssynpunkt och där behovet

av kunskaper om utrikes förhållanden framstår som särskilt angelägna.

Mot denna bakgrund bör Säkerhetspolisen få använda signalspaning för att motverka:

1. underrättelseverksamhet som kan antas bedrivas av främmande makt eller av organisation som huvudsakligen finns utomlands, om verksamheten är riktad mot Sverige eller svenska intressen eller på annat sätt berör Sverige,
2. annat hot mot rikets säkerhet,
3. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
4. internationell terrorism, eller
5. annan grov organiserad brottslighet.

Med begreppet motverka avses både att förebygga och uppdaga samt att avstyra och utreda den brottliga verksamheten. De uppräknade fallen är uttömmande. Det rör sig om två fall av allvarliga hot mot rikets säkerhet samt tre fall som inte är kopplade till skyddet av den säkerheten. Signalspaningen får bara användas för att motverka de uppräknade verksamheterna.

Gemensamt för de ovan nämnda punkterna är att de avser ansvarsområden inom Säkerhetspolisen där det framstår som särskilt angeläget för Säkerhetspolisen att kunna skaffa sig kunskap och följa utvecklingstendenser med avseende på utrikes förhållanden eller där sådan kunskap till och med framstår som avgörande för en framgångsrik verksamhet. Det är vidare områden där ett fullbordat brott allvarligt skulle komma att skada Sverige eller svenska intressen. Det är slutligen områden där Sverige har ett väl etablerat samarbete med andra länder för att öka kunskapen och motverka brott.

Punkt 1 gäller underrättelseverksamhet som kan antas bedrivas av främmande makt eller av organisation som huvudsakligen finns utomlands. Med främmande makt avses annan stat eller sammanslutning av stater. Med organisation som huvudsakligen finns utomlands avses t.ex. multinationella företag, väpnade rörelser i andra länder eller exilorganisationer av olika slag. Om sådana bedriver underrättelseverksamhet, kan således Säkerhetspolisen få använda signalspaning mot dessa, om övriga förutsättningar för det är upp-

fyllda. Det förutsätts att underrättelseverksamheten är olovlig. För att signalspaning ska få sättas in krävs emellertid också att underrättelseverksamheten riktar sig mot Sverige, svenska intressen eller på annat sätt berör vårt land. Till svenska intressen hör bl.a. sådant som rör Sveriges förhållande till andra stater, svenskt medlemskap i internationella organisationer, verksamhet som bedrivs i sådana organisationer som Sverige är medlem i, svenska eller delvis svenska företags verksamhet och svenska medborgare. Också underrättelseverksamhet som sker utomlands men riktar sig mot utländska medborgare (statslösa) med hemvist i Sverige får anses vara en verksamhet som riktar sig mot svenska intressen eller i vart fall berör Sverige. Om underrättelseverksamhet riktar sig mot enbart annan stat eller enbart utländska intressen men helt eller delvis bedrivs i Sverige, får verksamheten också anses beröra Sverige. Så kan t.ex. vara fallet om en annan stats underrättelseorganisationer har i Sverige stationerade medarbetare som bedriver underrättelseinhämtning mot en tredje stat.

Punkt 2 gäller ”annat allvarligt hot mot rikets säkerhet”. Subversiv verksamhet som hotar statsskicket kan vara ett exempel.

Punkt 3 gäller signalspaning i syfte att motverka spridning av massförstörelsevapen. Med massförstörelsevapen avses biologiska, kemiska och nukleära vapen.

Punkt 4 gäller internationell terrorism. Rent inhemsk terrorism omfattas således inte. Terrorismen ska ha en utländsk anknytning. Inte heller omfattas terrorism som rör enbart ett utländskt land. En befrielserörelse i ett land kan därför inte – även om landets regim skulle beteckna den som en terroristorganisation – träffas av bestämmelsen i denna punkt.

Punkt 5 gäller ”annan grov organiserad brottslighet”. Brottsligheten ska alltså både vara grov och organiserad. Ordet annan markerar att även verksamhet som omfattas av punkterna 1–4 kan (men inte behöver) utgöra grov organiserad brottslighet.

Gemensamt för punkterna 3–5 är att hotet i dessa stycken inte behöver vara riktat mot Sverige. Under punkt 3 faller således fall där ämnen som kan användas för tillverkning av massförstörelsevapen ska säljas från ett land i Östeuropa till ett land i Asien. På motsvarande sätt faller under punkt 4 ett fall där en grupp som finns i t.ex. ett baltiskt land planerar en terrorattack i ett sydeuropeiskt land eller deltar i understödet för en sådan attack. Också när det gäller den grova organiserade brottsligheten kan det röra sig om brottslighet som inte har anknytning till Sverige.

Orsaken är att Sverige ingår i ett internationellt samarbete på dessa områden som syftar till att stödja varandras strävan att bekämpa dessa företeelser.

7.4.3 Krav på proportionalitet

Som jag konstaterat tidigare är signalspaning till sin natur en integritetskränkande inhämtningsmetod. Detta är också skälet till att användningen av signalspaning inom polisen måste begränsas i olika avseenden och att tillämpningsområdet måste preciseras.

Det är emellertid enligt min mening inte tillräckligt att enbart uppställa generella kriterier som en begränsning av användningen. Det måste därtill prövas om signalspaningen är motiverad utifrån de omständigheter som råder i varje enskilt fall. Det bör därför, i likhet med vad som gäller enligt lagen om signalspaning i försvarsunderrättelseverksamheten, inför varje inhämtning genom signalspaning göras en proportionalitetsbedömning. För det fall syftet med signalspaningen inte väger klart tyngre än det integritetsintrång som spaningen kan medföra bör signalspaning inte få genomföras.

Detsamma bör gälla om det syftet kan tillgodoses på ett mindre ingripande sätt, t.ex. genom annan typ av spaning eller underrättelseinhämtning. Det bör klargöras att hemlig teleavlyssning, med den precision som användningen av det tvångsmedlet kräver i fråga om en identifierad teleadress, bör anses vara mindre integritetskränkande än signalspaning. Vid signalspaning finns inte alltid en teleadress och spaningen kommer därmed inte att få samma precision som hemlig teleavlyssning. För det fall en sådan teleadress finns bereds signalspaningsmyndigheten, såvitt gäller spaning i tråd, ändå tillgång till hela den signalbärare i vilken kommunikationen sker (se avsnitt 7.11.3 om signalbärare). Detta innebär att signalspaningsmyndigheten ges tillgång till fler signaler än vad som behövs för att nå syftet med spaningen. Mot den bakgrunden bör således signalspaning inte få förekomma om det är möjligt att nå samma syfte med användning av hemlig teleavlyssning. Detta bör gälla även i de fall den hemliga teleavlyssningen skulle kunna verkställas utanför Sverige med hjälp av ett annat lands myndigheter med stöd av överenskommelser om internationell rättslig hjälp.

Det resonemanget innebär också att så snart ett annat, mindre ingripande medel kan användas, t.ex. när spaningen har möjliggjort

att en skäligen misstänkt person och dennes teleadress har kunnat identifieras, skall signalspaningen upphöra och en annan metod, t.ex. hemlig teleavlyssning, i stället användas.

Av betydelse för bedömningen av om användningen av metoden väger klart tyngre än det integritetsintrång som spaningen kan medföra är naturligtvis också brottslighetens art. Det bör inte komma i fråga att använda metoden med avseende på brottslighet som inte framstår som mycket allvarlig och där inga andra medel står till buds. I praktiken torde metoden komma till användning, utom i de fall som rör Säkerhetspolisens ansvarsområden, endast vid grov organiserad brottighet med internationella kopplingar och i undantagsfall även vid annan mycket grov brottslighet där andra metoder saknar verkan. Det är också i dessa fall som metoden hittills har använts.

Utgångspunkten bör således vara att signalspaning inom polisen ska användas enbart i de fall det framstår som absolut nödvändigt för att fullgöra uppdraget och där inga andra, mindre integritetskränkande medel står till buds.

7.4.4 Utrikes förhållanden

Enligt mina direktiv ska jag undersöka behovet av underrättelser om utrikes förhållanden. Eftersom jag inte har för avsikt att inom ramen för detta utredningsuppdrag lämna förslag kring polisens närspaning (se avsnitt 7.1.9) bör den nu föreslagna regleringen begränsas till utrikes förhållanden. Mitt förslag om signalspaning inom polisen kommer därmed att på den punkten harmoniera med den lagstiftning som redan finns kring signalspaning inom försvarsunderrättelseverksamheten.

I ett antal länder jag studerat har signalspaningen begränsats på så sätt att den enbart får avse utländska medborgare. I den mån det uppdagas att en medborgare i det egna landet, var helst i världen denne befinner sig, är föremål för signalspaning ska spaningen omedelbart avbrytas och det inhämtade materialet förstöras. En sådan avgränsning framstår som svår att genomföra och efterleva i praktiken. Av de informationer som jag inhämtat från utländska signalspaningsorgan och organ som har till uppgift att övervaka signalspaningsorgan framgår att man i andra länder har haft praktiska svårigheter med tillämpningen av denna begränsning. Det framstår vidare som tveksamt om avgränsningen är ändamålsenlig – även egna

medborgare kan från utlandet planera brott mot rikets säkerhet, terroristbrott eller vara delaktiga i grov organiserad brottslighet. Ett sådant hot framstår knappast som mindre allvarligt än om planeringen utförs av en utländsk medborgare.

Det är vidare inte möjligt att begränsa polisens signalspaning genom att ange tillämpningsområden som typiskt sett enbart berör utrikes förhållanden på sätt som gjorts inom ramen för försvarsunderrättelseverksamheten. Brott som planeras och begås utomlands av utländska medborgare utan någon koppling till Sverige är ju knappast föremål för intresse från svensk polis sida, utom i de fall kriminaliteten omfattas av ett internationellt samarbete som Sverige deltar i.

I stället bör den nödvändiga avgränsningen göras från tekniska utgångspunkter. För att signalspaning ska få användas av polisen bör därför gälla att antingen avsändaren eller mottagaren av ett meddelande ska befinna sig utanför Sverige. De förutsättningar som måste gälla för att polisen ska få använda signalspaning blir därmed antingen att en person i Sverige kommunicerar med någon person i utlandet eller att de personer som kommunicerar med varandra båda befinner sig i utlandet.

I de fall både avsändare och mottagare finns i Sverige bör polisen i stället uteslutande vara hänvisade till annan typ av spaning eller, för det fall en förundersökning pågår, de straffprocessuella tvångsmedlen, t.ex. hemlig teleavlyssning.

Det har från många håll under lagstiftningsarbetet kring signalspaningen inom försvarsunderrättelseverksamheten framförts betänkligheter kring möjligheten att tekniskt avgränsa spaningen till utländska förhållanden. Enligt den kritik som har framförts kan exempelvis internettrafik mellan två personer passera Sveriges gräns även om såväl avsändare som mottagare befinner sig i Sverige.

Invändningen är väl värd att beakta, men är på intet sätt ny i fråga om polisens verksamhet. Samma typ av invändning kan göras gällande i fråga om flera av de straffprocessuella tvångsmedlen. Vid hemlig teleavlyssning avlyssnas en viss teleadress. Således kommer alla de personer som använder sig av teleadressen, t.ex. de medlemmar i den misstänktes hushåll som använder telefonen för egna ärenden och alla de personer som i olika syften ringer till teleadressen, att avlyssnas. Vid hemlig kameraövervakning filmas en viss plats. Alla de personer som befinner sig på den platsen kommer därmed också att filmas, oavsett deras koppling till den

aktuella brottsutredningen. Åtgärderna träffar därmed med nödvändighet mer än vad som motiveras utifrån polisens behov.

Det är mot denna bakgrund väsentligt att det finns klara och tydliga regler i fråga om på vilket sätt och i vilken omfattning den information som polisen erhåller från signalspaningen får användas och bevaras. När det gäller det nu beskrivna kravet på utrikes förhållanden ska därför stå klart att om signaler som inte får inhämtas, dvs. trafik mellan en avsändare och en mottagare som båda befinner sig i Sverige, av någon anledning inte har kunnat avskiljas tidigare ska upptagningen eller uppteckningen av innehållet i meddelandet förstöras så snart det upptäcks. En motsvarande bestämmelse har i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201 s. 40 ff) föreslagits beträffande signalspaning i försvarsunderrättelseverksamheten.

7.5 Ytterligare begränsningar i fråga om signalspaning i tråd

Förslag: Polisen ska få använda signalspaning i tråd endast om de förutsättningar som gäller för användning av hemlig teleavlyssning föreligger i det enskilda fallet, dock endast om hemlig teleavlyssning av något skäl inte kan anordnas.

Säkerhetspolisen ska därtill få använda signalspaning i tråd i underrättelsesyfte under i stort samma förutsättningar som gäller för signalspaning i etern.

7.5.1 Inledande synpunkter

Som framgått ovan har avlyssning av telefonsamtal i tråd och annan trådburen kommunikation så länge metoden har funnits ansetts som synnerligen integritetskränkande. Hemlig teleavlyssning och hemlig teleövervakning är straffprocessuella tvångsmedel som kringgärdas av tydliga begränsningar och rättssäkerhetsgarantier.

Medan signalspaning i etern har ansetts fri att bedriva utan särskilt lagstöd har signalspaning avseende trådbunden kommunikation hittills inte varit tillåten över huvud taget. Förslagen ovan kring de generella förutsättningarna för signalspaning innebär därmed en avsevärd begränsning av möjligheterna till signalspaning

i etern jämfört med de förutsättningar för sådan spaning som har rått hittills. Det finns anledning att kringgärda signalspaning i tråd med än större begränsningar.

För det första är avlyssning av trådbunden kommunikation redan reglerad genom bestämmelser om straffprocessuella tvångsmedel, dvs. hemlig teleavlyssning och hemlig teleövervakning. Som jag framhållit tidigare får det inte förekomma att polisen använder signalspaning i syfte att kringgå de bestämmelserna. Signalspaning i tråd måste därför regleras på ett sådant sätt att metoden inte missbrukas.

För det andra ger signalspaning i tråd tillgång till en betydligt större mängd information än spaning i etern. Det måste därför finnas tydliga begränsningar i fråga om hur informationen får samlas in i syfte att säkerställa att enbart den kommunikation som polisen avser att signalspana mot blir föremål för spaningen.

Av samma skäl som anförts ovan beträffande signalspaning i etern finns därtill skäl att skilja mellan signalspaning i tråd inom Säkerhetspolisens och den övriga polisens verksamhetsområden.

En första utgångspunkt är för mig att – om polisen över huvud taget ska få tillgång till signalspaning i tråd – det inte kan komma i fråga annat än i samband med bekämpningen allvarliga hot mot nationell eller internationell säkerhet eller mot mycket grov brottslighet i övrigt. Kravet att det ska gälla mycket grov brottslighet gäller redan i dag för de hemliga tvångsmedlen, dvs. hemlig teleavlyssning och hemlig teleövervakning, hemlig rumsavlyssning och hemlig kameraövervakning. För de nämnda hemliga tvångsmedlen gäller olika krav på allvaret i de brott för vilka de kan användas. Hemlig rumsavlyssning får som huvudregel användas vid utredning av brott för vilka är stadgat ett straffminimum om fyra år. För användning av hemlig teleavlyssning och hemlig kameraövervakning gäller ett straffminimum för brottet om två år, medan hemlig tele-övervakning som huvudregel kan användas för brott för vilket är stadgat minst sex månaders fängelse.

Att jämföra signalspaning med de hemliga tvångsmedlen låter sig i och för sig inte göras fullt ut. De hemliga tvångsmedlen används inom ramen för förundersökningar och riktar sig mot skäligen misstänkta individer. Signalspaningen har i stället sin stora användning i underrättelseverksamheten och är inte nödvändigtvis inriktade på enskilda individer. I den mån signalspaningen är inriktad på enskilda individer syftar spaningen ofta till att identifiera dessa för

att därefter kunna gå vidare med en brottsutredning, eventuellt med användning av hemliga tvångsmedel.

Om signalspaning i tråd ska tillåtas får den mot denna bakgrund inte vara så begränsad att syftet med spaningen skulle gå om intet. Inte heller får spaningen ges ett sådant generellt tillämpningsområde att enskilda individer utan starka skäl utsätts för polisens övervakning.

7.5.2 Tillämpningsområdet generellt

Som konstaterats tidigare är signalspaning en mycket integritetskränkande spaningsmetod. Detta gäller särskilt spaningen i trådbunden trafik. En noggrann prövning måste därmed göras avseende behovet av sådan signalspaning.

Det är min uppfattning att Rikskriminalpolisen och polismyndigheterna har ett klart mer begränsat behov av signalspaning i tråd än vad som är fallet med Säkerhetspolisen. Verksamheten inom Rikskriminalpolisen och polismyndigheterna är i huvudsak reaktiv och inriktad på utredning av begångna brott. Därtill är verksamheten till en mycket liten del inriktad på utländska förhållanden. För den typ av brott där signalspaning trots allt har använts, t.ex. grova narkotikabrott med internationell anknytning, finns dessutom andra, mindre ingripande metoder att nå information.

Efter vad jag har erfarit är de hemliga tvångsmedel som kan användas såväl preventivt som inom ramen för en förundersökning (se avsnitt 2.3) i stort tillfyllest för den verksamhet som bedrivs vid Rikskriminalpolisen och polismyndigheterna. Det har inte anförts några bärande skäl att ge polisen några ytterligare befogenheter på dessa områden.

Endast i ett avseende – bortsett från behovet att använda signalspaning i tråd för Säkerhetspolisens arbete med att bekämpa allvarliga hot mot nationell och internationell säkerhet – tycks det finnas ett behov av att kunna använda signalspaning i tråd för polisens verksamhet. Det är när förutsättningarna för att använda hemlig teleavlyssning är uppfyllda, men sådan avlyssning av någon anledning inte kan komma till stånd i praktiken. Det rör sig alltså då om så grov brottslighet att lagstiftaren redan i dag har ansett att det är befogat att avlyssna telekommunikation i tråd.

För att polisen i så fall ska kunna använda sig av signalspaning i tråd måste därmed krävas att det finns en skäligen misstänkt person

och att omständigheterna är sådana att det hade varit möjligt för en domstol att bevilja tillstånd till hemlig teleavlyssning.

Ett typexempel på när signalspaning i tråd i så fall skulle kunna komma till användning skulle därmed vara att en person som är skäligen misstänkt för grovt narkotikabrott befinner sig utomlands i ett land där en i Sverige beslutad hemlig teleavlyssning inte skulle kunna verkställas med stöd av det landets myndigheter. Ett annat exempel skulle kunna vara att den skäligen misstänkte person befinner sig utomlands och att polisen saknar kännedom om dennes teleadress. I båda dessa fall är det enligt min mening rimligt att kunna säkerställa avlyssningen genom signalspaning i tråd. Som nämnts ovan (avsnitt 7.4.3) bör hemlig teleavlyssning och hemlig teleövervakning anses som mindre ingripande metoder. Det innebär att så snart de metoderna kan användas – t.ex. genom att den misstänkte för en tid reser till och uppehåller sig i ett land där en hemlig teleavlyssning eller hemlig teleövervakning kan verkställas med hjälp av det landets myndigheter – ska signalspaningen avbrytas till förmån för andra, mindre ingripande metoder.

Att bestämmelserna om hemlig teleavlyssning inte ska kunna kringgås medför också att de andra regelverk som kan komma att aktualiseras i samband med en hemlig teleavlyssning måste beaktas i tillämpliga delar. Bestämmelserna i lagen (2000:562) om internationell rättslig hjälp i brottmål berör bl.a. hemlig teleavlyssning såsom dessa frågor har reglerats i 2000–års EU-konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (se närmare prop. 2004/05:144). Beträffande andra länder än konventionsstaterna ska naturligtvis eventuella folkrättsliga principer och förpliktelser kring brottsutredande verksamhet beaktas.

Det bör framhållas att användningen av signalspaning i tråd i praktiken kan komma att begränsas avsevärt mot bakgrund av svårigheten att använda information från signalspaning som bevisning i en rättegång (se avsnitt 7.12).

Med ledning av vad jag nu har anfört har jag kommit fram till att signalspaning i tråd bör få användas för bekämpning av brott som är så allvarliga att i det enskilda fallet de i redan gällande rätt uppställda förutsättningarna för att polisen ska få använda hemlig teleavlyssning är uppfyllda, dock att signalspaningen ska få användas endast om i det enskilda fallet det av något skäl i praktiken inte kan anordnas hemlig teleavlyssning.

Jag vill i detta sammanhang nämna att jag övervägt om det från rättssäkerhets- eller integritetsskyddssynpunkt skulle kunna finnas något hinder mot att signalspaning i tråd under de nu av mig föreslagna förutsättningarna får användas för polisens behov för att utreda brott. Jag har emellertid svårt att se att något sådant hinder skulle föreligga. Om man som jag gjort begränsar det till fall där förutsättningarna i redan gällande rätt för att använda hemlig teleavlyssning föreligger, har ju lagstiftaren redan i dag ansett att den berörda teletrafiken ska få avlyssnas för polisens behov. Att samma teletrafik nu får avlyssnas genom signalspaning medför enligt min mening inte annat än att avlyssningen av den ifrågavarande teletrafiken sker på ett annat sätt. I andra länder, vars lagstiftning jag studerat (t.ex. Kanada och Tyskland) görs ingen uppdelning i lagstiftningen mellan signalspaning och hemlig teleavlyssning. Båda företeelserna anses utgöra en och samma lagtekniska metod, benämnd avlyssning av telekommunikation (i Kanada ”interception of telecommunications” och i Tyskland ”Überwachung der Telekommunikation”). En förutsättning för detta resonemang är förstås att polisen inte får tillgång till mer information genom att teletrafiken avlyssnas med hjälp av signalspaning än om den avlyssnas med hjälp av hemlig teleavlyssning. Hur detta ska säkerställas återkommer jag till i avsnitt 7.8. Av det som anförs där följer i själva verket att polisen när inhämtningen sker genom signalspaning får tillgång till mer begränsad information än om samma inhämtning sker genom hemlig teleavlyssning. Vid den sistnämnda metoden får polisen nämligen tillgång till innehållet i all trafik som går i den avlyssnade kommunikationen, medan vid signalspaningen polisen endast får tillgång till det som är relevant för utredning av det brott som föranlett avlyssningen.

7.5.3 Särskilt om Säkerhetspolisens underrättelseinhämtning

Samma argument som anförts ovan kring Säkerhetspolisens användning av signalspaning generellt (dvs. i praktiken spaning i etern) kan göras gällande vad gäller signalspaning i tråd. Vad som ovan anförts beträffande möjligheten att använda signalspaning i tråd inom den öppna polisen bör därmed gälla också för Säkerhetspolisen. Av väsentlig betydelse är att inte heller Säkerhetspolisen under några omständligheter kan tillåtas kringgå bestämmelserna om hemlig teleavlyssning.

Säkerhetspolisen bör därtill också få bedriva signalspaning i tråd i underrättelsesyfte, dvs. utan att syftet med spaningen är att skaffa bevisning mot enskilda misstänkta. Det är, som redogjorts för tidigare, inom detta område som Säkerhetspolisen bedriver huvuddelen av sin verksamhet och där myndighetens kunskap om utrikes förhållanden är av avgörande betydelse för att uppdaga och motverka säkerhetshotande verksamhet. Tillämpningsområdet bör därvid vara detsamma som när det gäller Säkerhetspolisens signalspaning i etern.

På en punkt bör emellertid användningen av signalspaning i tråd begränsas. När det gäller Säkerhetspolisens verksamhet med att motverka grov organiserad brottslighet bör signalspaning i tråd få användas endast till den del sådan brottslighet utgör ett hot mot det demokratiska systemet i Sverige eller rättssystemet här, s.k. systemhotande brottslighet. För den grova organiserade brottsligheten i övrigt kan göras gällande samma argument mot en alltför generös reglering av signalspaning i tråd som anförts ovan beträffande polisen i övrigt, dvs. dels att värdet av signalspaning framstår som begränsat, dels att de hemliga tvångsmedel som kan användas inom ramen för en förundersökning får anses tillgodose polisens behov.

7.5.4 Begränsningar i övrigt

Vad som ovan beträffande signalspaning i etern har föreslagits om krav på proportionalitet bör gälla även för signalspaning i tråd.

Även vad som för signalspaning i etern har föreslagits kring utrikes förhållanden bör gälla för signalspaning i tråd. Den tekniska avgränsningen bör vad gäller signalspaning i tråd utformas så att spaningen endast får avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör. Samma begränsning har gjorts för signalspaning i tråd i försvarsunderrättelseverksamheten (2 § lagen [2008:717] om signalspaning i försvarsunderrättelseverksamhet).

Det finns också skäl att polisen, i det stora flöde av information som är trådbunden, inte får tillgång till annan information än sådan som omfattas tillstånd till signalspaning. Även om polisen inte skulle ha rätt att använda sådan information kan blotta tillgången väcka farhågor om missbruk. Det har mot denna bakgrund betydelse vem som utför spaningen och att det inte är polisen själv som sorterar ut den information som får användas. Jag återkommer till den frågan i avsnitt 7.8

7.6 Automatiserad inhämtning m.m.

7.6.1 Automatiserad inhämtning

Förslag: Inhämtning av signaler i tråd ska ske automatiserat.

Regeringen har beträffande signalspaningen i tråd inom försvarsunderrättelseverksamheten anfört att på grund av den oerhörda mängd trafik som förmedlas genom signaler i elektronisk form måste inhämtningen ske automatiserat med hjälp av datorer. En manuell inhämtning är enligt regeringen betydligt mer resurskrävande och medför dessutom ökade risker för intrång i den personliga integriteten. För sådan signalspaning gäller därför enligt 3 § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet att den ska ske automatiserat. Vad gäller signalspaning i etern har regeringen anfört att det kan finnas ett behov av manuell inhämtning, även om inhämtningen även där i huvudsak sker automatiserat (prop. 2006/07:63 s. 76).

Det saknas anledning att göra en annan bedömning kring kravet på automatiserad inhämtning vid signalspaning i tråd när det gäller polisens signalspaning. Ett motsvarande krav bör därför gälla även på det området.

7.6.2 Användning av sökbegrepp

Förslag: All automatiserad inhämtning ska ske med användning av sökbegrepp, oavsett om den automatiserade inhämtningen sker i tråd eller i etern.

Allmänt om sökbegrepp

Regeringen har beträffande automatiserad inhämtning inom försvarsunderrättelseverksamheten anfört att sådan inhämtning i teorin skulle kunna äga rum genom att all förekommande trafik inhämtas och lagras för senare bearbetning. Detta skulle enligt regeringen emellertid innebära ett oproportionerligt intrång i den personliga integriteten och skulle därtill ställa närmast orealistiska krav på kapacitet för lagring av information. För sådan signal-

spaning gäller därför enligt 3 § andra stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet att den ska ske med användning av sökbegrepp i syfte att säkerställa att inhämtning sker endast av information som kan ha betydelse för verksamheten (prop. 2006:07:63 s. 76 f).

Det saknas även på denna punkt skäl att göra en annan bedömning beträffande signalspaning inom polisens verksamhet. Även för den signalspaningen bör därför gälla att all automatiserad inhämtning ska ske med användning av sökbegrepp.

Hur sökbegreppen används är av grundläggande betydelse för allmänhetens förtroende för signalspaningsverksamheten. Den debatt som föregått lagstiftningen kring signalspaningen har till stor del haft sin utgångspunkt i möjligheten för statliga organ att fritt spana mot såväl etern som trådbundna kommunikationer och risken för att myndigheterna skulle kunna komma att missbruka den möjligheten. Kravet på användning av sökbegrepp är ett sätt att reducera mängden information som myndigheterna inhämtar och behandlar samt att motverka missbruk genom att möjliggöra kontroller i efterhand. Det är mot denna bakgrund viktigt att sökbegreppen utformas med en sådan precision att omotiverade intrång i den personliga integriteten undviks. Det är därmed en central uppgift för tillståndsorganet (se avsnitt 7.7) att noggrant pröva om de sökbegrepp som anges i varje enskilt fall har den precision som krävs för att minimera risken för att annan trafik än den som avses med tillståndet blir föremål för inhämtning.

Sökbegrepp som är hänförliga till enskild person

Av 4 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet följer att en inriktning av signalspaningen inte får avse endast en viss fysisk person. När det gäller att använda sökbegrepp som är hänförliga till en enskild person gäller enligt lagen om signalspaning i försvarsunderrättelseverksamhet att sådana sökbegrepp får användas endast om det är av synnerlig vikt för verksamheten. Användningen av sökbegrepp som är hänförliga till enskilda personer förutsätts därmed vara mycket restriktiv i den verksamheten (3 § andra stycket).

Signalspaningen för polisens räkning har en annan inriktning än vad som gäller för försvarsunderrättelseverksamheten. Verksamheten inom såväl Säkerhetspolisen som den övriga polisen syftar till

att förebygga brottslig verksamhet. I de fall ett brott har begåtts är det polisens uppgift att utreda brottet och att samla bevis i en sådan omfattning att det är möjligt att lagföra de individer som gjort sig skyldiga till en brottslig gärning. Även om föremålen för polisens intresse skulle vara organisationer eller grupperingar av olika slag, är det ytterst enskilda individer som måste granskas och förmås avbryta sin brottsliga verksamhet. Säkerhetspolisens och den övriga polisens uppdrag är mot denna bakgrund betydligt mer inriktat mot enskilda individer än vad som är fallet inom försvarsunderrättelseverksamheten. Även om användningen av sökbegrepp som är hänförliga till enskilda individer bör ske med restriktivitet även när det gäller signalspaning för polisens räkning skulle en alltför restriktiv reglering komma att göra signalspaningen verkningslös.

Det är mot denna bakgrund min uppfattning att det vid signalspaning för polisens räkning inte bör vara förbjudet att inrikta spaningen mot endast en fysisk person. Jag föreslår vidare att det ska vara möjligt för polisen att använda sökbegrepp som är hänförliga till enskilda personer i de fall det hade varit möjligt för polisen att använda sig av hemlig teleavlyssning, antingen enligt rättegångsbalken eller enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. I dessa fall har polisen identifierat en misstänkt person och brottet är av den svårighetsgrad som krävs för hemlig teleavlyssning. Att i dessa fall använda sökbegrepp som är hänförliga till den misstänkta personen är enligt min mening godtagbart från integritetssynpunkt.

För att använda sökbegrepp som är hänförliga till enskilda personer i övrigt bör krävas att det föreligger särskilda skäl. Även om kravet är lägre ställt än inom försvarsunderrättelseverksamheten markeras med en sådan bestämmelse att det inte får komma i fråga att rutinmässigt använda den typen av sökbegrepp. Användningen måste i stället motiveras särskilt i varje enskilt fall.

7.6.3 Tillgång till signalbärare

Förslag: Signalspaningsmyndigheten ska få tillgång till enbart de signalbärare som behövs för att fullgöra uppdraget.

Det följer av den lagstiftning som riksdagen redan beslutat om när det gäller signalspaning i försvarsunderrättelseverksamheten att

signalspaningen i tråd ska möjliggöras genom att operatörerna ska överföra all gränsöverskridande trafik till ett antal s.k. samverkanspunkter. All gränsöverskridande trådbunden trafik kommer därmed att koncentreras till dessa samverkanspunkter och göras tillgänglig för signalspaning. Det rör sig om en oerhört stor mängd information. Även om signalspaningsmyndigheten av rättsliga skäl är förhindrade att ta del av all den information som passerar samverkanspunkterna har från många håll uttryckts en oro över att myndigheten tekniskt skulle ha en sådan möjlighet. Oron får därmed snarast betraktas som en farhåga att det beskrivna systemet skulle kunna komma att missbrukas.

I propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201 s. 33 ff) föreslås mot denna bakgrund att den rättsliga begränsning i hanteringen av information som följer av såväl den nu gällande som den föreslagna lagstiftningen ska kompletteras med tekniska begränsningar. Förslaget i propositionen har sin grund i den politiska överenskommelsen mellan de partier som ingår i regeringen (se avsnitt 4.2.3), av vilken framgår att signalspaningsmyndigheten ska få tillgång till endast de ”trafikstråk” som domstolen bestämmer.

Enligt vad som föreslås i propositionen ska signalspaningsmyndigheten inte ges tillgång till annan trafik än den som är nödvändig för att spaningen i varje enskilt fall ska kunna genomföras. I syfte att uppnå en sådan begränsning föreslås att signalspaningsmyndigheten i samband med tillståndsförfarandet endast ska få tillgång till de s.k. signalbärare avseende signaler i tråd som behövs för att utföra uppdraget. Det är därefter enbart trafiken i just den signalbäraren som blir föremål för signalspaning i tråd genom att signalspaningsmyndigheten i den fibern genomför den automatiserade sökning med hjälp av sökbegrepp som beskrivits i avsnittet ovan.

Enligt uppgift passerar den aktuella trafiken Sveriges gräns i färre än 50 olika kablar. Varje kabel innehåller ett antal fibrer, antingen 48 fibrer per kabel eller 96 fibrer per kabel. Med signalbärare avses en enskild fiber. Att begränsa möjlighet att avlyssna trafiken vid samverkanspunkterna till enskilda fibrer skulle därmed avsevärt begränsa mängden information som signalspaningsmyndigheten skulle få tillgång till i varje enskilt fall.

Enligt förslaget i propositionen ska frågan om vilka signalbärare som signalspaningsmyndigheten ska få tillgång avgöras av den domstol som ska avgöra tillståndsfrågan. Kontrollen över vilka signalbärare som signalspaningsmyndigheten rent tekniskt ska få

tillgång till ska enligt förslaget emellertid tillkomma kontrollmyndigheten. Det är således enligt förslaget kontrollmyndigheten som kommer att ha den samlade tekniska kontrollen över samverkanspunkterna och den trafik som passerar där. Kontrollmyndigheten kommer att bevilja signalspaningsmyndigheten tillgång till endast de signalbärare avseende signaler i tråd som domstolen har bestämt.

De tekniska begränsningar som kommer att gälla för signalspaningsmyndigheten inom ramen för försvarsunderrättelseverksamheten bör gälla även för den signalspaning som myndigheten bedriver för polisens räkning. Systemet med tillstånd till särskilda signalbärare avseende signaler i tråd bör därför gälla även vid signalspaning för polisens räkning. Jag återkommer till frågan om hur den frågan bör hanteras praktiskt (se avsnitt 7.11.3).

En ytterligare begränsning såvitt gäller polisens tillgång till den information som inhämtas genom signalspaning är att inhämtningen och sorteringen av relevant information, dvs. sådan information som omfattas av tillstånd till signalspaningen, utförs av annan än polisen. Jag återkommer till den frågan i avsnitt 7.8.

7.7 Tillståndsprövningen

7.7.1 Bakgrund

Enligt lagen (2008:717) om signalspaning i förvarsunderrättelseverksamhet gäller att det krävs tillstånd för en myndighets närmare inriktning av signalspaning. Regeringens eller Regeringskansliets inriktning omfattas inte av kravet på tillstånd. Tillstånd beslutas av Signalspaningsnämnden (5 och 6 §§).

Av överenskommelsen mellan de partier som ingår i regeringen (se avsnitt 4.2.3) framgår att tillstånd till signalspaning i stället ska prövas av domstol. Propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) innehåller mot den bakgrunden ett förslag om att införa en sådan domstolsprövning (se prop. s. 42 ff).

I propositionen föreslås att en specialdomstol, Försvarsunderrättelsedomstolen, inrättas för ändamålet. Domstolen ska enligt förslaget ha som enda uppgift att pröva ansökningar om tillstånd till signalspaning och domstolens beslut ska inte gå att överklaga. Domstolens ordförande föreslås anställas som ordinarie domare

och till domstolen ska vidare knytas högst två vice ordförande som ska vara lagfarna och ha erfarenhet av tjänstgöring som domare. Därtill ska domstolen bestå av högst sex andra ledamöter med särskild kunskap om förhållanden av betydelse för domstolens verksamhet. Domstolen föreslås vara domför med ordföranden och två andra ledamöter.

Enligt förslaget i propositionen ska all signalspaning omfattas av tillståndsprövningen, alltså även sådan signalspaning som har sin bakgrund i regeringens inriktning. Det är emellertid inte de myndigheter som står bakom inriktningen av signalspaningen som ska ansöka om tillstånd, utan i stället signalspaningsmyndigheten.

Regeringen föreslår i propositionen vidare att ett integritetsskyddsombud (en motsvarighet till de offentliga ombud som deltar vid prövningen av tillstånd till vissa straffprocessuella tvångsmedel) ska beakta integritetsskyddsintresset i mål vid domstolen.

Domstolens avgöranden föreslås inte kunna överklagas.

7.7.2 Allmänna utgångspunkter

Bedömning: Samma domstol bör pröva ärenden om signalspaning i försvarsunderrättelseverksamheten och i polisens verksamhet. Starka skäl talar mot att det för det ändamålet inrättas en specialdomstol.

För det fall det blir aktuellt även för Säkerhetspolisen och den övriga polisen att bedriva signalspaning är det min uppfattning att även sådan signalspaning bör vara beroende av domstols tillstånd. Såväl kompetens- som resursskäl talar för att det bör vara samma domstol som ger tillstånd i de båda fallen. Dess uppdrag skulle därmed bli att pröva ansökningar om tillstånd till signalspaning såväl inom ramen för försvarsunderrättelseverksamheten som inom Säkerhetspolisens och den övriga polisens verksamhet. Jag redogör emellertid nedan för en alternativ modell för tillståndsprövningen som, om den skulle bli verklighet, skulle komma att omfatta såväl den signalspaning som utförs för polisens räkning som signalspaningen inom försvarsunderrättelseverksamheten.

Förslaget att inrätta en specialdomstol avviker markant från den linje som statsmakterna hittills har intagit och som går ut på att

undvika att ha specialdomstolar. Principen har hittills varit att i möjlig mån avskaffa specialdomstolar och att inte inrätta några nya.

För en specialdomstol talar att ämnesområdet är mycket speciellt och kan kräva särskild sakkunskap. Även den omständligheten att sakområdet måste omgärdas av stark sekretess kan möjligen tala för en specialdomstol. Å andra sidan handlägger såväl de allmänna domstolarna som de allmänna förvaltningsdomstolarna många frågor av starkt specialiserad karaktär och också många frågor som måste omgärdas med stark sekretess. Det har inte påvisats att detta skulle vara något problem för dessa domstolar. Som exempel på speciella uppgifter som dessa domstolar har och som kräver särskild sakkunskap kan nämnas miljömål, patentmål och utlänningsrätt. Som exempel på områden som kräver stark sekretess kan nämnas spionmål, ärenden om hemliga tvångsmedel och ärenden rörande tillämpning av lagen (1991:572) om särskild utlänningskontroll.

Mot en specialdomstol talar flera skäl. Ett är att en specialdomstol som blir så liten att den bara innehåller en anställd domare (och två ersättare på uppdrag) kommer att kunna ifrågasättas på den grunden att regeringen får möjlighet att styra vem som ska handlägga de integritetskänsliga frågorna om tillstånd till signalspaning. Annorlunda blir det om man – som när det gäller t.ex. spionmålen i Stockholms tingsrätt – låter en stor domstol ta hand om uppgiften. Det blir då domstolen själv som bestämmer vilken eller vilka av dess domare som ska ta hand om handläggningen av signalspaningsmålen. Det kommer också att bli möjligt för domstolen att med vissa mellanrum byta ut någon eller några av de domare som handlägger dessa mål. Vidare finns fördelen att målkategorin kan fördelas på flera domare. Från demokrati- och rättssäkerhetssynpunkt är det en bättre lösning att välja en större, befintlig domstol och inte en specialdomstol.

Ett annat skäl att inte välja en specialdomstol är att det i dag kan vara svårt att avgöra vilken arbetsbörda det kommer att bli i uppgiften att pröva ansökningar om tillstånd till signalspaning. Inom ramen för en större befintlig domstol kan den uppgiften samordnas med andra uppgifter och en sådan lösning blir därför mer flexibel.

En nackdel med en specialdomstol är också att det finns en risk för att en sådan domstol – som bara har uppgiften att pröva ansökningar om tillstånd till signalspaning – efter en tid kan komma att bli så nära förbunden med verksamheten att dess självständiga prövning av tillståndsfrågan kan komma att ifrågasättas. Det gäller särskilt

som endast få domare kommer att vara verksamma i domstolen. I en större domstol där den ifrågavarande uppgiften bara är en av flera och där domarna kan vara flera och med jämna mellanrum skifta arbetsuppgifter är risken klart mindre att den nu nämnda nackdelen ska uppstå.

Avsikten med de förslag som lagts fram i propositionen är att stärka allmänhetens förtroende för att rättssäkerhet och skydd för personlig integritet beaktas när frågor om tillstånd till signalspaning prövas. Det är därför angeläget att prövningen görs av en instans som kan stå oberoende från såväl statsmakterna som de myndigheter som har intresse av signalspaningen. Det vore olyckligt om prövningsinstansen får en utformning som inte kommer att kunna få allmänhetens förtroende.

Det finns enligt min mening således tunga skäl för att inte välja lösningen med en specialdomstol. I stället bör uppgiften att pröva ansökningar om tillstånd till signalspaning anförtros åt en redan existerande större domstol.

En fördel med detta skulle också vara att det skulle finnas en överklagandemöjlighet. Detta är något som skulle kunna vara av betydelse om och när Europadomstolen för mänskliga rättigheter prövar om Sverige uppfyller Europakonventionens krav.

För den händelse lagstiftaren ändå skulle välja lösningen med en specialdomstol, bör den – med hänsyn till vad jag ovan anfört om att samma domstol bör ge tillstånd till signalspaning för polisens räkning – inte benämnas Försvarsunderrättelsedomstolen, utan förslagsvis Säkerhets- och underrättelsedomstolen eller annan neutral benämning.

7.7.3 Prövning i allmän förvaltningsdomstol

Förslag: Ärenden om tillstånd till signalspaning ska prövas av allmän förvaltningsdomstol. Besluten ska kunna överklagas.

Mot den bakgrund som anges ovan bör tillståndsprövningen äga rum inom den befintliga domstolsorganisationen. Närmast till hands ligger att välja en allmän förvaltningsdomstol. Domstolen bör vara tillräckligt stor för att de fördelar som beskrivs ovan kan förverkligas. Domstolen bör vidare vara så belägen geografiskt att ansökande myndigheter med kort varsel kan inställa sig i samband

med prövningen. Jag föreslår att uppgiften anförtros Länsrätten i Stockholms län.

Domstolens avgöranden bör kunna överklagas till Kammarrätten i Stockholm.

På grund av ärendenas speciella karaktär finns skäl att kringgärda domstolens prövning med särskilda åtgärder. Dessa åtgärder får ankomma på domstolen att genomföra, t.ex. angående förtur, speciallottning och jourtjänstgöring. Vidare finns skäl att kringgärda prövningen med särskilda arrangemang från säkerhetssynpunkt. En möjlighet bör även finnas för domstolen att vid behov knyta till sig experter. Jag har vid kontakter med ledningen för Kammarrätten i Stockholm försäkrat mig om att frågor av säkerhetskaraktär inte bedöms utgöra något problem vid ett eventuellt genomförande av mitt förslag.

Som jag anfört tidigare är det min uppfattning att det bör vara samma domstol som beslutar om tillstånd när det gäller signalspaning för polisens räkning som när det gäller signalspaning i försvarsunderrättelseverksamheten. En förutsättning för mitt förslag att det är Länsrätten i Stockholms län som ska pröva ansökningarna som första instans är därmed att lagstiftaren beslutar om den lösningen även inom ramen för det lagstiftningsarbete som redan är föremål för beredning.

Om en sådan lösning skulle väljas får det naturligtvis konsekvenser för domstolsväsendet i form av en ökad belastning och behov kan finnas av särregler kring handläggningen där, t.ex. i fråga om möjligheten att anlita experter. Det faller emellertid utanför mitt uppdrag att beträffande signalspaningen inom försvarsunderrättelseverksamheten göra sådana bedömningar. Att begränsa en sådan konsekvensanalys till att enbart avse sådana ärenden som rör polisens signalspaning framstår inte som meningsfullt, eftersom slutsatserna skulle komma att bygga på en tämligen begränsad del av de signalspaningsärenden som domstolen kommer att ha att hantera. Mitt förslag i denna del måste mot denna bakgrund bli föremål för en fortsatt beredning i Regeringskansliet där hänsyn kan tas till såväl signalspaningen i försvarsunderrättelseverksamheten som den signalspaning som föreslås i detta betänkande.

7.7.4 Medverkan av offentliga ombud

Förslag: Offentliga ombud ska medverka vid tillståndsprövningen.

Offentliga ombud ska i ärenden om hemlig teleavlyssning, hemlig kameraövervakning och hemlig rumsavlyssning bevaka enskildas integritetsintressen (se 27 kap. 26-30 §§ rättegångsbalken och 7 § lagen [2007:978] om hemlig rumsavlyssning).

De offentliga ombuden utses av regeringen och ska vara eller ha varit advokater eller ha varit ordinarie domare. Uppgiften är inte att företräda den misstänkte som tvångsmedlet är avsett att riktas emot, utan att företräda enskildas rätts- eller integritetsintressen i allmänhet. Ett offentligt ombud har för att fullgöra sitt uppdrag rätt att ta del av vad som förekommer i ärendet, att yttra sig i ärendet och att överklaga rättens beslut.

Det är min uppfattning att offentliga ombud bör medverka också vid prövningen av tillstånd till signalspaning. I konsekvens med att jag föreslår att ärendena ska avgöras av allmän förvaltningsdomstol är det min uppfattning att dessa ombud bör utgöras av de offentliga ombud som beskrivs ovan. Det saknas anledning att finna en särlösning för just ärenden om tillstånd till signalspaning. Ombuden får med den av mig föreslagna domstolslösningen en viktig uppgift i att kunna överklaga tillståndsbesluten.

Regeringen har i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201 s. 66 ff) föreslagit att det vid prövningen i den föreslagna specialdomstolen i stället ska medverka s.k. integritetsskyddsombud. Ombudens uppdrag ska vara desamma som de offentliga ombudens, med den viktiga skillnaden att med den domstolslösning som regeringen föreslagit kommer ombuden inte att ha möjlighet att överklaga tillståndsbesluten. Integritetsskyddsombuden föreslås utgöra en särskild kategori av ombud, skild från de offentliga ombuden. För det fall sådana integritetsskyddsombud skulle införas inom ramen för den föreslagna specialdomstolen bör samma lösning gälla för tillståndsärenden enligt den nu föreslagna lagen om signalspaning för polisens räkning.

7.7.5 Vem ska ansöka om tillstånd?

Förslag: Den myndighet som har behov av signalspaningen ska ansöka om tillstånd. Myndigheten ska biträdas av signalspaningsmyndigheten.

Förslagen i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201 s. 47 ff) innebär som tidigare nämnts att det är signalspaningsmyndigheten som ska ansöka om tillstånd hos domstolen. Jag ställer mig tveksam till den lösningen, i vart fall såvitt avser signalspaning som utförs för polisens räkning.

När det gäller frågan om vilken myndighet som ska ansöka om tillstånd hos domstolen måste beaktas dels i vems intresse som signalspaningen ska genomföras, dels vilken typ av uppgifter som domstolen behöver som grund för sitt ställningstagande.

Signalspaning äger uteslutande rum i den inriktande myndighetens intresse, dvs. såvitt nu är aktuellt Säkerhetspolisens eller Rikskriminalpolisens. Signalspaningsmyndigheten bedriver således inte någon signalspaning utifrån egna behov av underrättelser.

De uppgifter som domstolen kommer att behöva som grund för sitt ställningstagande är av två typer.

Det rör sig å ena sidan om uppgifter som kan läggas till grund för domstolens behovs- och proportionalitetsbedömningar, dvs. vilket behov den inriktande myndigheten har av signalspaningen och varför det behovet inte kan tillgodoses på ett mindre ingripande sätt. Bäst lämpad att presentera ett underlag i dessa frågor är den myndighet som har behov av signalspaningen, dvs. såvitt nu är aktuellt Säkerhetspolisen eller Rikskriminalpolisen.

Å andra sidan har domstolen också behov av upplysningar av teknisk karaktär, främst frågor kring vilken eller vilka signalbärare som signalspaningsmyndigheten behöver ha tillgång till och vilka sökbegrepp som det finns behov av att använda. Det är en typ av frågor som endast signalspaningsmyndigheten har kompetensen att besvara.

Resonemanget medför att domstolen har behov av uppgifter och upplysningar från såväl den myndighet som har behov av signalspaningen som den myndighet som ska utföra spaningen. Båda myndigheterna måste således medverka i förfarandet. Det är min uppfattning att den grundläggande sakfrågan i ett tillståndsärende, dvs. behovet av att genomföra signalspaningen, bör vara

avgörande för vilken myndighet som ska stå bakom en ansökan. Det bör mot den bakgrunden, såvitt gäller den signalspaning som här är aktuell, vara Säkerhetspolisen eller Rikskriminalpolisen som ska stå bakom ansökan till domstolen.

För att säkerställa att domstolen får ett fullgott underlag även vad gäller de tekniska förutsättningarna bör det åligga signalspaningsmyndigheten att biträda den ansökande myndigheten och, i förekommande fall, tillsammans med den myndigheten uppträda inför domstolen.

Det är min uppfattning att det förfarande jag nu har föreslagit bör gälla oberoende av vilken lösning som väljs inom ramen för försvarsunderrättelseverksamheten. Det skulle därmed kunna komma att tillämpas två olika ansökningsförfaranden, ett för den signalspaning som bedrivs på uppdrag av polisen och ett annat för den signalspaning som bedrivs i förvarsunderrättelseverksamheten.

7.7.6 Beslut i brådskande fall

Förslag: Interimistiska tillstånd till signalspaning ska kunna meddelas av signalspaningsmyndighen på begäran av den myndighet som har behov av åtgärden.

Enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska som nämnts tidigare ansökningar om tillstånd prövas av Signalspaningsnämnden. I brådskande fall får signalspaning genomföras utan att nämnden fattar beslut om tillstånd. Den aktuella inriktningen ska då i stället omedelbart anmälas till nämnden. Nämnden ska därefter, om den finner att förutsättningar för tillstånd saknas, omedelbart underrätta signalspaningsmyndigheten som i sin tur omedelbart ska avbryta verksamheten (5 § tredje stycket).

I propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) föreslås, som framgått ovan, att Signalspaningsnämnden ersätts av Försvarsunderrättelsedomstolen. För brådskande fall föreslås i propositionen att tillstånd till signalspaning i stället får lämnas av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver. Åtgärden ska därefter omedelbart anmälas skriftligen till Försvarsunderrättelsedomstolen, som skyndsamt ska pröva ärendet (prop. s. 61 ff).

Det saknas skäl att ifrågasätta att det i fråga om signalspaning finns behov av att kunna fatta beslut skyndsamt. En sådan möjlighet bör därför finnas. Möjligheten bör inte bara gälla då ett nytt tillstånd behövs, utan också om ett befintligt tillstånd snabbt behöver kompletteras med exempelvis ett nytt sökbegrepp eller tillgång till en ny signalbärare.

En nackdel med förslaget i propositionen är att det är samma myndighet som har till uppgift att ansöka om tillstånd till signalspaningen, som har att verkställa beslut om signalspaning och som fattar interimistiska beslut. det gäller även om avsikten är att en av regeringen särskilt utsedd tjänsteman vid signalspaningsmyndigheten ska fatta de interimistiska besluten. En sådan ordning framstår enligt min mening inte som den bästa för att trygga rättssäkerheten och den gagnar inte en hög trovärdighet i verksamheten.

Med mitt förslag ovan om att den myndighet som har behov av signalspaningen ska vara sökande i domstolen ges förutsättningar för en bättre ordning kring de beslut som kräver skyndsam handläggning. I brådskande fall har då den myndighet som har behov av att få signalspaning utförd – i de nu aktuella fallen Säkerhetspolisen eller Rikskriminalpolisen – att vända sig till signalspaningsmyndigheten som kan fatta ett beslut om tillstånd till spaningen. Åtgärden ska därefter genast anmälas till domstolen.

En anmälan till kontrollmyndigheten bör göras för det fall verkställigheten av ett interimistiskt beslut om signalspaning hunnit avbrytas innan en anmälan till domstolen har kunnat ske. Lagstiftaren har nyligen gjort det ställningstagandet att en sådan anmälan till tillsynsorganet ska ske vad gäller interimistiska beslut enligt lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott, om verkställigheten av beslutet avbrutits innan beslutet prövats av domstol. Avsikten med skyldigheten att göra en sådan anmälan är att förebygga missbruk och upprätthålla allmänt förtroende för möjligheten att fatta interimistiska beslut. En motsvarande bestämmelse har också i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201 s. 65) föreslagits beträffande signalpaning i försvarsunderrättelseverksamheten.

7.7.7 Närmare om tillståndens omfattning m.m.

Förslag: En ansökan om tillstånd ska innehålla grunderna för ansökan samt upplysningar om signalbärare, sökbegrepp, den tid som ansökan avser och eventuella omständigheter i övrigt.

Tillstånd till signalspaning får ges för högst tre månader och får därefter förlängas med högst tre månader i taget. Tillståndet ska begränsas till de signalbärare och sökbegrepp som behövs för att uppnå syftet med spaningen. Domstolen får förena tillståndet med de villkor som behövs för att begränsa intrånget i enskildas personliga integritet.

Utgångspunkter

I lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, enligt vilken Signalspaningsnämnden ska fatta beslut om tillstånd, finns endast ett fåtal bestämmelser om innehållet i ansökningar respektive tillstånd. I propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) har föreslagits kompletterande bestämmelser på området, bestämmelser som har sin bakgrund i det i samma proposition redovisade förslaget om inrättande av Försvarsunderrättelsedomstolen.

Det saknas skäl att beträffande signalspaning för polisens räkning ha bestämmelser kring innehållet i ansökningar och tillstånd som på något avgörande sätt avviker från de bestämmelser som gäller vid signalspaning i försvarsunderrättelseverksamheten. Mitt lagförslag avviker emellertid rent lagtekniskt från det förslag som redovisats i propositionen. I propositionen föreslås bestämmelser om under vilka förutsättningar ett tillstånd får lämnas. I fråga om mitt lagförslag är dessa förutsättningar emellertid med självklarhet de som gäller för att polisen ska få bedriva signalspaning och som redan följer av rekvisit i lagen. Någon bestämmelse motsvarande de som finns i den nämnda propositionen föreslås därför inte här.

Ansökningar

Den ansökande myndigheten, såvitt här är aktuellt antingen Säkerhetspolisen eller Rikskriminalpolisen, ska i ansökan redogöra för grunderna för ansökan, dvs. en redogörelse för på vilka grunder

myndigheten anser att domstolen ska bevilja ansökan. I detta ligger att myndigheten måste redogöra för de omständigheter som domstolen måste bedöma för att kunna bevilja tillstånd, framför allt sådana omständigheter som ligger till grund för domstolens behovs- och proportionalitetsbedömningar.

Den ansökande myndigheten ska vidare redovisa de signalbärare som myndigheten finner nödvändiga för att utföra spaningen och de sökbegrepp som myndigheten avser att använda. Beträffande dessa båda punkter är det nödvändigt att den ansökande myndigheten biträds av signalspaningsmyndigheten.

Slutligen ska i ansökan anges den tid under vilken spaningen bedöms behöva pågå samt eventuella omständigheter i övrigt.

Tillstånd

I tillståndet ska anges den tid under vilken signalspaningen ska få bedrivas. Enligt 5 § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet gäller att tillstånd för signalspaning får ges för högst sex månader och att det därefter kan förlängas med högst sex månader i taget.

Den tid under vilken signalspaning för polisens räkning ska få bedrivas behöver inte med nödvändighet vara densamma som för signalspaning inom försvarsunderrättelseverksamheten. Som en jämförelse kan nämnas att tiden för hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning inte får överstiga en månad från dagen för beslutet (se 27 kap. 21 § andra stycket rättegångsbalken). Samma tidsgräns gäller för hemlig rumsavlyssning.

Som tidigare har redogjorts för syftar signalspaningen inom polisen i huvudsak till att kartlägga företeelser, organisationer och grupper samt enskilda individer i syfte att uppdaga brottslig verksamhet. Sådan kartläggning sker inom ramen för underrättelseverksamheten och har ofta ett tämligen långsiktigt syfte. Den tid under vilken signalspaning i ett visst syfte kan bedrivas får därmed inte sättas alltför kort. Å andra sidan talar integritetsintresset för att signalspaning för polisens räkning inte ska kunna få pågå under alltför lång tid utan att domstolen på nytt ges en möjlighet att bedöma behovet. Att tillåta en alltför lång tid riskerar att påverka förtroendet för verksamheten negativt. Jag föreslår mot denna bakgrund att signalspaningen inte ska få pågå längre tid än tre månader

från dagen för beslutet och att tillståndet därefter kan förlängas med högst tre månader i taget.

Vid en prövning av frågan hur lång tid ett tillstånd ska gälla i det enskilda fallet får naturligtvis den ovan beskrivna proportionalitetsprincipen (avsnitt 7.4.3) stor betydelse. Tiden kan komma att variera från ärende till ärende. Likaså kan tiden mellan olika typer av ärenden variera. Exempelvis kan nog signalspaning i underrättelsesyfte ofta bedömas kräva längre tid än signalspaning i en förundersökning med en skäligen misstänkt person.

Vad gäller innehållet i tillståndet i övrigt bör detsamma gälla som föreslås i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201 s. 59 ff). Domstolen ska därvid i tillståndet ange de signalbärare avseende signaler i tråd som signalspaningsmyndigheten ska få tillgång till, de sökbegrepp som får användas och de villkor i övrigt som domstolen anser behövs för att begränsa intrånget i enskildas personliga integritet.

7.8 Vem ska utföra signalspaningen?

Förslag: Försvarets radioanstalt ska utföra signalspaning kring utrikes förhållanden för polisens räkning.

7.8.1 Inledning

Jag ska enligt mina direktiv överväga olika alternativa lösningar för att verkställa underrättelseinhämtningen. Mot bakgrund av de ställningstaganden kring polisens behov av signalspaning som redovisas ovan innebär uppdraget i denna del att överväga vem som ska utföra den signalspaning som polisen har behov av. Det finns tre alternativa lösningar:

1. signalspaning genom Försvarets radioanstalts försorg,
2. signalspaning genom polisens försorg och
3. amarbete med utländska myndigheter.

7.8.2 Signalspaning genom Försvarets radioanstalts försorg

För att låta Försvarets radioanstalt utföra signalspaningen åt polisen talar att Försvarets radioanstalt redan besitter det kunnande och innehar den tekniska utrustning som behövs för att utföra uppdraget. Myndigheten har utfört signalspaning för polisens räkning i flera årtionden. Polisen och Försvarets radioanstalt har därmed ett väl etablerat samarbete.

Försvarets radioanstalt har genom de ändringar som beslutats inom ramen för försvarsunderrättelseverksamheten redan det kunnande och den teknik som krävs för att biträda polisen enligt de förslag som jag lämnar i detta betänkande.

7.8.3 Signalspaning genom polisens försorg

Varken Säkerhetspolisen eller den övriga polisen har i dag tillgång till det kunnande eller den teknik som krävs för att själv bedriva signalspaning. Att låta bygga upp en sådan förmåga inom polisen är självfallet möjligt, men skulle kräva avsevärda investeringar. Det kunnande och den teknik som behövs är desamma som i dag redan finns vid Försvarets radioanstalt. En sådan lösning skulle därmed innebära att polisen parallellt med Försvarets radioanstalt skulle bygga upp en organisation med samma förmåga som Försvarets radioanstalt redan har.

Det är min uppfattning att en sådan lösning inte är försvarbar från kostnads- och effektivitetssynpunkt. Den skulle därtill kräva många år av förberedelser och ytterligare år av löpande verksamhet för att nå upp till den kompetensnivå som Försvarets radioanstalt besitter.

Ett annat viktigt skäl att inte låta polisen själv bedriva signalspaning behandlas i avsnitt 7.8.6.

7.8.4 Anlitande av utländska myndigheter

En möjlighet som, i vart fall teoretiskt, skulle kunna stå till buds för att täcka polisens underrättelsebehov om utrikes förhållanden är att de svenska myndigheterna söker information och biträde från utländska underrättelsetjänster, säkerhetsunderrättelsetjänster eller signalspaningsmyndigheter.

Det bör inledningsvis framhållas att det är oklart om ett sådant alternativ är praktiskt genomförbart. Förvisso finns ett internationellt samarbete mellan olika länders underrättelsetjänster, säkerhetsunderrättelsetjänster, polismyndigheter och signalspaningsmyndigheter. Samarbetet syftar emellertid till ett ömsesidigt utbyte av information som samtliga deltagande myndigheter i längden drar nytta av. Att ensidigt och på kontinuerlig basis låta myndigheter i ett land överlämna underrättelseinformation till myndigheter i ett annat land framstår som främmande.

Den information de svenska myndigheterna skulle få inom ramen för ett sådant samarbete kan också vara svår att värdera. Varje land har sina egna intressen och sina egna prioriteringar. Varje underrättelse från en utländsk myndighet måste därför värderas och bedömas med viss försiktighet.

Det finns vidare en risk att svenska myndigheter i sitt samarbete med utländska myndigheter tvingas avslöja alltför mycket av sina egna prioriteringar och intresseområden. Verksamheten skulle därmed kunna komma att skadas och förmågan att fullgöra statsmakternas uppdrag skulle kunna komma att minska.

Att låta utländska myndigheter tillgodose den svenska polisens underrättelsebehov medför slutligen också stora negativa konsekvenser såvitt avser möjligheten till insyn och kontroll.

Mot denna bakgrund är det min bestämda uppfattning att det inte bör komma i fråga att täcka polisens underrättelsebehov kring utländska förhållanden genom ett internationellt samarbete.

7.8.5 Sammanfattande synpunkter

Att låta Försvarets radioanstalt biträda polisen med signalspaning framstår som den enda rimliga lösningen. De båda andra alternativen är behäftade med så stora nackdelar att de knappast framstår som genomförbara. Alternativet med Försvarets radioanstalt är däremot snabbt genomförbart och har i sammanhanget rimliga ekonomiska konsekvenser.

Förslaget att det är Försvarets radioanstalt som ska bedriva signalspaningen på polisens begäran är självfallet begränsat till signalspaning som omfattas av detta utredningsuppdrag, dvs. signalspaning kring utrikes förhållanden. Att polisen i andra sammanhang kan ha behov av och rätt att bedriva signalspaning, exempelvis s.k. närspan-

ing, är en fråga som faller utanför mitt uppdrag (se avsnitt 7.1.9 angående Polismetodutredningens pågående uppdrag).

7.8.6 Ytterligare skäl för den föreslagna lösningen

Inte bara effektivitetsskäl talar för att Försvarets radioanstalt ska utföra signalspaningen för polisens räkning. Även rättssäkerhetsskäl och betydelsen av att stävja varje misstanke om missbruk talar för en sådan lösning.

I Tyskland får s.k. strategisk kommunikationsövervakning i tråd mot utländska förhållanden utföras endast av utrikesunderrättelsetjänsten (BND), som är den myndighet i Tyskland som också tekniskt genomför avlyssningen. I Kanada finns däremot en särskild signalspaningsmyndighet som tekniskt genomför sådan spaning för andra myndigheters räkning.

Om polisen i Sverige själv skulle få tekniskt genomföra avlyssningen, skulle polisen rent faktiskt komma att besitta mer information än som omfattas av det ändamål för vilket avlyssningen beviljats. Vid inhämtning i tråd skulle visserligen bara den information som befordras i den tillståndsgivna tråden (signalbäraren) komma att inhämtas, men eftersom det i en och samma tråd går inte bara den trafik som polisen fått tillstånd att inhämta utan också annan trafik, skulle en hel del ”överskottsinformation” komma att finnas hos polisen. Även om polisen inte skulle ha rätt att ta del av den sistnämnda, skulle förhållandet att informationen fanns i polisens hand enligt min mening på goda grunder kunna kritiseras.

Genom att föreskriva att polisen inte själv ska få genomföra inhämtningen begränsas polisens tillgång till sådan information som tillståndet att avlyssna avser. Endast denna information ska av Försvarets radioanstalt överföras till polisen. Övrig information stannar hos Försvarets radioanstalt. Härigenom förhindras att polisen får tillgång till en omfattande avlyssning av de internationella kommunikationer som i tråd passerar Sveriges gräns. Polisen får i stället bara tillgång till den information som den ska ha enligt det tillstånd som domstolen givit. Ett motsvarande resonemang kan föras även beträffande avlyssning i etern. Det bör ankomma på domstolen att i samband med tillståndsgivningen avgöra vilka uppgifter som ska få lämnas till polisen.

7.8.7 Teknik- och kompetensutveckling m.m.

Av 1 § tredje stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet följer att signalspaningsmyndigheten får bedriva signalspaning 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 verksamhet enligt den lagen.

Syftet med sådan signalspaning är att tillgodose Försvarets radioanstalts egna behov av teknik- och kompetensutveckling. Inhämtningen är en förutsättning för att signalspaningen ska kunna bedrivas.

Försvarets radioanstalt bör ha en sådan möjlighet även enligt den nu föreslagna lagen om signalspaning för polisens behov. För sådan inhämtning bör i tillämpliga delar gälla samma förutsättningar som för signalspaning enligt den föreslagna lagen i övrigt.

Tillstånd till signalspaning för dessa ändamål bör sökas av Försvarets radioanstalt, inte av polisen.

För den typ av signalspaning som har beskrivits här, dvs. signalspaning i syfte att utveckla teknik och kompetens, behöver Försvarets radioanstalt vidare etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer Regeringen bestämmer närmare om förutsättningarna för ett sådant samarbete. En sådan möjlighet följer av 9 § lagen om signalspaning i försvarsunderrättelseverksamhet och en motsvarande möjlighet bör följa även av den nu föreslagna lagstiftningen.

7.9 Granskning och förstöring av uppgifter, m.m.

7.9.1 Generellt om granskning och förstöring

Förslag: Upptagningar eller uppteckningar som gjorts vid signalspaning ska omedelbart granskas av polisen. De får bevaras endast under vissa angivna förutsättningar och ska därefter förstöras.

Vad som av signalspaningsmyndigheten inhämtas vid signalspaning kan delges polisen på olika sätt. Delgivningen kan ske genom att

s.k. råmaterial överlämnas. Delgivningen kan vidare ske genom underrättelserapporter där materialet varit föremål för signalspaningsmyndighetens bearbetning och analys. Vilken form som väljs är naturligtvis beroende av de behov som polisen har och de alternativ som i varje fall är möjliga att åstadkomma. Valet av redovisningsform kan också ha sin grund i behovet hos signalspaningsmyndigheten att i olika avseenden hemlighålla sina metoder och sin förmåga. Viktigt är att redovisningen till polisen aldrig får innehålla annan information än den som omfattas av domstolens tillstånd.

För upptagningar eller uppteckningar som gjorts vid signalspaning för polisens räkning bör gälla samma typ av granskningsskyldighet som gäller i samband med användning av hemlig teleavlyssning och andra hemliga tvångsmedel (se exempelvis 27 kap. 24 § rättegångsbalken).

Mot denna bakgrund bör gälla att upptagningar eller uppteckningar som har inhämtats genom signalspaning ska granskas av polisen snarast möjligt.

I vilken utsträckning materialet ska bevaras är beroende av i vilka syften det kan komma till användning. I de delar materialet är av betydelse från brottsutredningssynpunkt ska det bevaras till dess förundersökningen lagts ned eller, om åtal väcks, målet har avgjorts slutligt. I de delar upptagningarna eller uppteckningarna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott.

När ingen av de två omständigheter som anges ovan för att bevara materialet föreligger ska det förstöras.

Det finns en risk att den förstöringsskyldighet som beskrivs ovan kan komma att kollidera med andra bestämmelser som reglerar behandlingen av uppgifter i polisens brottsbekämpande verksamhet. För polisens del måste därför gälla att om det har kommit fram uppgifter som får behandlas i register eller på annat sätt enligt annan lagstiftning, främst polisdatalagen (1998:622), utgör den nu föreslagna lagstiftningen inte något hinder mot att uppgifterna behandlas enligt den lagstiftningen.

7.9.2 Särskilda grunder för förstöring

Förslag: Upptagningar eller uppteckningar som gjorts vid signalspaning ska omedelbart förstöras om innehållet avser viss kommunikation som bör åtnjuta särskilt skydd.

Det finns i samband med signalspaning behov av en än mer långtgående förstöringsskyldighet än den som föreslås ovan. I avsnitt 7.4.4 har exempelvis redogjorts för den förstöringsskyldighet som föreslås gälla när det i efterhand visar sig att både avsändare och mottagare till de inhämtade signalerna vid inhämtningen har befunnit sig i Sverige.

I 7 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet finns därutöver bestämmelser om under vilka förutsättningar uppgifter som inhämtats vid signalspaning ska förstöras. Av bestämmelsen följer att upptagning eller uppteckning av uppgifter som inhämtats genom signalspaning omgående ska förstöras om innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för försvarsunderrättelseverksamheten,
2. avser uppgifter för vilka tystnadsplikt gäller enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen eller som omfattas av förbudet att efterforska meddelare, eller
3. omfattar samtal mellan en misstänkt och dennes försvarare.

Bestämmelsen har motiverats utförligt i lagförarbetena (prop. 2006/07:63 s. 103 ff). Därutöver har i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201 s. 79 ff) föreslagits att bestämmelsen utökas på det sättet att en upptagning eller uppteckning omgående ska förstöras också om innehållet avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för ändamål som anges i lagen.

Den ovan angivna punkten 1 saknar relevans såvitt avser signalspaning för polisens räkning. I övrigt finns det ett värde i att grunderna för förstöringsskyldigheten är desamma vid signalspaning i försvarsunderrättelseverksamheten som vid signalspaning för polisens räkning. En sådan överensstämmelse bör gynna allmänhetens förtroende för verksamheten.

7.9.3 Hantering av personuppgifter

Förslag: Vid behandling av personuppgifter ska i första hand bestämmelserna i den nu föreslagna lagen tillämpas. I övrigt ska de regelverk tillämpas som annars reglerar behandlingen av personuppgifter vid respektive myndighet.

I samband med polisens signalspaning kommer att behandlas personuppgifter såväl inom polisen som vid signalspaningsmyndigheten. Både för verksamheten inom polisen och vid Försvarets radioanstalt finns särskilda bestämmelser om behandling av personuppgifter. Det centrala regelverket för polisens del är polisdatalagen (1998:622), medan bestämmelser om personuppgiftsbehandlingen vid Försvarets radioanstalt följer av lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Till de båda lagarna finns förordningar.

Den nu föreslagna lagen om signalspaning i polisens verksamhet innehåller vissa bestämmelser om behandling av personuppgifter, t.ex. bestämmelserna om sökbegrepp som är hänförliga till enskild person samt om granskning, bevarande och förstöring av uppgifter.

För behandling av personuppgifter vid polisens signalspaning bör i första hand de regler som följer av den nu föreslagna lagen tillämpas, såväl inom polisen som vid Försvarets radioanstalt. I övrigt bör vid respektive myndighet den lagstiftning tillämpas som normalt gäller för behandling av personuppgifter i den verksamheten, dvs. för polisens del huvudsakligen polisdatalagen och för Försvarets radioanstalts del lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

7.9.4 Överlämnande av underrättelser

Förslag: Uppgifter som inhämtats genom signalspaning för polisens räkning och som har betydelse för svensk utrikes-, säkerhets- och försvarspolitik ska kunna överlämnas till regeringen, Regeringskansliet och Försvarsmakten.

Signalspaning föreslås således få bedrivas såväl inom försvarsunderrättelseverksamheten som för polisens räkning. Som har framgått ovan (avsnitt 4.2) innebär den inriktning av signalspaningen inom försvarsunderrättelseverksamheten som regeringen föreslagit ett utökat mandat att ägna uppmärksamhet åt bl.a. internationell brottslighet.

Mot den bakgrunden är det självfallet av väsentlig betydelse att information som erhålls genom signalspaning i försvarsunderrättelseverksamheten kan överlämnas till polisen i den mån uppgifterna har betydelse för polisens verksamhet. En sådan möjlighet finns också enligt 2 § första stycket lagen (2000:130) om försvarsunderrättelseverksamhet.

På motsvarande sätt kan ett behov finnas av att till myndigheter utanför polisen överlämna information som inhämtats den signalspaning som utförs för polisens räkning. Det rör sig om information av betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, dvs. samma intressen som försvarsunderrättelseverksamheten ska stödja. Kretsen av mottagare till sådan information bör begränsas till dem som har rätt att inrikta den signalspaning som bedrivs inom försvarsunderrättelseverksamheten, dvs. enligt förslaget i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201 s. 31 ff) regeringen, Regeringskansliet och Försvarsmakten. Att informationen fritt kan överlämnas till regeringen är självklart. En särskild bestämmelse bör emellertid införas för att utan hinder av sekretess kunna överlämna sådan information till Regeringskansliet och Försvarsmakten.

Frågan om att på detta sätt överlämna information bör avgöras av Försvarets radioanstalt. Innan information överlämnas bör emellertid samråd alltid ske med Rikspolisstyrelsen genom antingen Säkerhetspolisen eller Rikskriminalpolisen beroende på informationens karaktär.

För det fall informationen har inhämtats inom ramen för en förundersökning bör självfallet gälla att informationen inte ska få överlämnas utan medgivande av förundersökningsledaren.

7.10 Underrättelseskyldighet

Bedömning: Någon skyldighet att underrätta enskilda i efterhand om att de varit föremål för signalspaning bör inte införas.

7.10.1 Bakgrund

I lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet saknas bestämmelser om underrättelseskyldighet, dvs. en skyldighet att i efterhand underrätta en enskild om att han eller hon varit föremål för signalspaning.

De partier som ingår i regeringen har emellertid i den politiska överenskommelsen uttalat att en sådan skyldighet ska införas. Mot den bakgrunden innehåller propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) ett sådant förslag (prop. s. 84 ff).

I propositionen föreslås att om det vid signalspaning har använts sökbegrepp som är direkt hänförliga till en viss fysisk person ska den person som sökbegreppen avser underrättas om detta. En underrättelse ska lämnas så snart det kan ske utan men för försvarsunderrättelseverksamheten, dock senast en månad efter det att det inhämtningsuppdrag som föranlett inhämtningen avslutades. En underrättelse får enligt förslaget skjutas upp om sekretess hindrar att underrättelsen lämnas. har det på grund av sekretess inte kunnat lämnas någon underrättelse inom ett år från det att inhämtningsuppdraget avslutades behöver någon underrättelse inte lämnas. Slutligen föreslås att en underrättelse inte ska lämnas om inhämtningen uteslutande avser främmande makts förhållanden eller förhållanden mellan främmande makter.

Syftet med att lämna en sådan underrättelse till enskilda personer är framför allt att den enskilde ska få möjlighet att bedöma vilket integritetsintrång som åtgärden har inneburit och att reagera mot vad han eller hon kan anse ha varit en rättstridig åtgärd.

7.10.2 Förhållandena i den brottsbekämpande verksamheten

Sedan den 1 januari 2008 gäller en underrättelseskyldighet för de brottsbekämpande myndigheterna i förhållande till enskild som under en förundersökning har varit föremål för hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning (27 kap. 31 § rättegångsbalken) samt hemlig rumsavlyssning (15 § lagen [2007:978] om hemlig rumsavlyssning).

Underrättelseskyldigheten begränsas av flera undantag. Om uppgifterna omfattas av sekretess ska underrättelsen skjutas upp till dess att sekretessen inte längre gäller och får helt underlåtas om det på grund av sekretess inte har kunnat lämnas någon underrättelse inom ett år. Vidare är förundersökningar beträffande vissa brott helt undantagna, vilket innebär att Säkerhetspolisens verksamhetsområde inte omfattas av underrättelseskyldigheten. Som skäl för undantaget anförde regeringen bl.a. att verksamhetsområdet genomgående är av särskilt känsligt slag och att det inom ramen för Säkerhetspolisens verksamhet regelmässigt pågår långvariga utredningar som inte avgränsas av enskilda förundersökningar och att en underrättelseskyldighet skulle försvåra Säkerhetspolisens deltagande i internationellt samarbete (prop. 2006/07:133 s. 50).

7.10.3 Underrättelseskyldighet vid signalspaning?

Jag vill inledningsvis kommentera förslaget i propositionen. I förslaget anges att det är den ”person som sökbegreppet avser” som ska underrättas om signalspaningen. Förslaget framstår som tveksamt. Denna person behöver ju inte själv ha varit utsatt för något intrång i sina förtroliga kommunikationer. Det är ju i stället den som utsatts för ett sådant intrång som har intresse av att bli underrättad. Om syftet är att avlyssna kommunikationen mellan personerna A och B när de talar om personen X kan uppgifter som är hänförliga till X användas som sökbegrepp. Med propositionens förslag är det därmed X som ska underrättas om att signalspaning förekommit, inte A och B vars kommunikation har blivit avlyssnad.

Det kan därtill noteras att utgångspunkterna för den föreslagna underrättelseskyldigheten inte går ihop med propositionens förslag beträffande tillsynsorganets utredningsskyldighet (prop. 2008/09:201 s. 91). En sådan utredning från tillsynsorganets sida ska nämligen

enligt propositionens förslag avse om den enskildes kommunikation har utsatts för signalspaning.

Oavsett detaljerna i förslaget kan det ifrågasättas om det i flertalet fall finns någon praktisk möjlighet att identifiera den som utsatts för intrång. Därtill kommer att det kan ta ganska lång tid innan underrättelse kan lämnas, vilket har betydelse för preskription av skadeståndskrav och åtal m.m., något som påverkar den enskildes möjlighet att i praktiken använda en underrättelse som utgångspunkt för att uppnå Europakonventionens krav på tillgång till ett effektivt nationellt rättsmedel. Slutligen kommer en sådan underrättelseskyldighet att behöva förses med så omfattande undantag att den riskerar att uppfattas som en chimär, vilket inte gynnar tilltron till regelverket och verksamheten.

Någon underrättelseskyldighet till enskilda med anledning av att det förekommit signalspaning förekommer inte heller i de länder jag har studerat. Den i propositionen föreslagna konstruktionen har i samband med mina besök utomlands snarare mötts med förvåning.

Vad som nu anförts leder till slutsatsen att det är tveksamt om någon underrättelseskyldighet alls bör föreligga vid signalspaning. I stället bör övervägas att ge varje enskild person rätt att begära en kontroll av om han eller hon har utsatts för signalspaning och om denna i så fall har skett i enlighet med lag eller annan författning, således en rätt att begära kontroll som går något längre än motsvarande förslag i propositionen. Jag återkommer till den frågan i avsnitt 7.11.1.

Ledamöterna i den referensgrupp som har biträtt mig i utredningsarbetet har överlag efterlyst att bestämmelser om underrättelseskyldighet införs i den föreslagna lagen, inte minst mot bakgrund av att en sådan skyldighet har föreslagits också beträffande signalspaning i försvarsunderrättelseverksamheten. Om lagstiftaren skulle besluta i enlighet med propositionens förslag vad gäller signalspaningen inom försvarsunderrättelseverksamheten och en motsvarande bestämmelse skulle efterlysas såvitt avser signalspaning för polisens räkning skulle en sådan bestämmelse kunna utformas enligt följande.

X § Om signalspaning skett med stöd av 5 § första stycket, gäller för signalspaningen vad som föreskrivs om hemlig teleavlyssning i 27 kap. 31–33 §§ rättegångsbalken. I stället för uppgift om teleadress ska uppgift lämnas om sådana använda sökbegrepp som är direkt hänförliga till den person som underrättas.

Om signalspaning skett med stöd av 5 § andra stycket, gäller för signalspaningen vad som föreskrivs om hemlig teleavlyssning i 16–18 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. I stället för uppgift om teleadress ska uppgift lämnas om sådana sökbegrepp som är direkt hänförliga till den person som underrättas.

Vad som föreskrivs i första och andra styckena gäller även vid annan signalspaning än sådan som sker i tråd, om signalspaningen sker inom ramen för en förundersökning och görs mot någon som är skäligen misstänkt för brott eller om den görs mot någon som det finns särskild anledning att anta kommer att utöva sådan brottslig verksamhet som avses i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

7.11 Insyn och kontroll

7.11.1 Tillsynen över polisens signalspaning

Förslag: Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn över polisens signalspaning.

Om Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden påbörjade sin verksamhet den 1 januari 2008. Verksamheten regleras i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Nämnden består av högst tio ledamöter som utses av regeringen för en tid av högst fyra år. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet.

Nämnden ska, såvitt här är av intresse, utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och därmed sammanhängande verksamhet samt Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (1998:622). Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i enlighet med lag eller annan författning.

Tillsynen omfattar således verksamhet där hemliga tvångsmedel, såsom hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning, används. Att tillsynen även avser med tvångsmedelsanvändningen ”sammanhängande verksamhet” innebär att

både själva avlyssningen eller övervakningen och den vidare hanteringen av upptagningarna, såsom hur överskottsinformation används eller förstörs, liksom fullgörandet av reglerna om underrättelseskyldighet, omfattas av tillsynen. Även den brottsbekämpande verksamhet som föregår och ligger till grund för ansökan om tvångsmedlet omfattas. Tillsynen är avgränsad till ”brottsbekämpande myndigheters” användning av metoderna. Det innebär att domstolarnas handläggning av och beslut i ärenden om tillstånd till användning av hemliga tvångsmedel inte omfattas av nämndens tillsyn. De brottsbekämpande myndigheterna är för närvarande Rikspolisstyrelsen, Säkerhetspolisen, polismyndigheterna, Åklagarmyndigheten och Ekobrottsmyndigheten samt även Tullverket, Kustbevakningen och Skatteverket. Användningen av hemliga tvångsmedel berör Åklagarmyndigheten, Ekobrottsmyndigheten, Säkerhetspolisen, den öppna polisen och Tullverket (jfr. prop. 2006/07:133 s. 79 f).

Nämnden utför sin tillsyn genom inspektioner och andra undersökningar. I uppdraget ingår att uttala sig om konstaterade förhållanden och om behovet av förändringar i verksamheten. Nämnden ska vidare verka för att brister i lag eller annan författning avhjälps.

Nämnden är skyldig att på begäran av enskild kontrollera om han eller hon har utsatts för sådana tvångsmedel och därmed sammanhängande verksamhet eller varit föremål för sådan personuppgiftsbehandling som omfattas av nämndens tillsyn. Nämnden ska underrätta den enskilde om att kontrollen har utförts.

Nämnden har rätt att av de myndigheter som omfattas av tillsynen få de uppgifter och det biträde som nämnden begär. Skyldigheten att lämna nämnden de uppgifter som den begär omfattar också domstolar och de myndigheter som inte omfattas av tillsynen.

Nämndens beslut får inte överklagas.

Av 22 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden följer vidare att för det fall nämnden i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska nämnden anmäla det förhållandet till Åklagarmyndigheten eller annan behörig myndighet. Om nämnden uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten ska nämnden anmäla det till Justitiekanslern. Om nämnden slutligen finner omständigheter som Datainspektionen bör uppmärksammas på ska nämnden anmäla det till inspektionen.

Tillsyn över polisens signalspaning

Av 10 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet jämförd med 2 § 4 förordningen (2007:852) med instruktion för Försvarets underrättelsenämnd är det Försvarets underrättelsenämnd som ansvarar för tillsynen avseende signalspaning i försvarsunderrättelseverksamheten. Nämnden har ett i grunden vidare mandat, nämligen att kontrollera försvarsunderrättelseverksamheten hos alla de myndigheter som bedriver sådan verksamhet och att granska behandlingen av personuppgifter i den verksamheten.

Av propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) framgår att regeringen har för avsikt att ombilda Försvarets underrättelsenämnd, bl.a. i syfte att ge myndigheten en mer rättslig karaktär. Myndigheten ska enligt regeringen därtill ges ett namn som bättre beskriver dess roll, Statens inspektion för försvarsunderrättelseverksamheten (prop. s. 95 ff).

Försvarets underrättelsenämnd har ett tydligt uppdrag inom försvarsunderrättelseverksamheten. Som jag redogjort för tidigare är det min uppfattning att den signalspaning som jag nu föreslår ska få bedrivas för polisens behov ska regleras skild från försvarsunderrättelseverksamheten. Det bör därmed inte komma i fråga att låta Försvarets underrättelsenämnd bedriva tillsyn över polisens signalspaningsverksamhet.

Mot bakgrund av det uppdrag som Säkerhets- och integritetsskyddsnämnden har enligt beskrivningen ovan faller det sig i stället naturligt att nämndens verksamhet utökas till att avse även den nu föreslagna signalspaningen för polisens räkning. Säkerhets- och integritetsskyddsnämndens uppdrag bör vara i stort detsamma vad gäller polisen signalspaning som redan gäller beträffande nämndens tillsyn i övrigt.

Särskilt viktig i sammanhanget framstår en skyldighet för nämnden att på begäran av enskild kontrollera om hans eller hennes kommunikation har inhämtats vid signalspaning eller om uppgifter om den enskilde har inhämtats vid signalspaning. En sådan kontroll bör särskilt inriktas på att kontrollera om förfarandet skett i enlighet med lag eller annan författning. En skyldighet bör föreligga för nämnden att underrätta den enskilde om att kontrollen har utförts. Som jag redogjort för ovan (avsnitt 7.10) föreslår jag att någon underrättelse till enskild i efterhand om att signalspaning förekommit inte bör införas. En vittgående skyldighet för ett till-

synsorgan att på en enskilds begäran kontrollera vad som förekommit är en förutsättning för att en sådan underrättelseskyldighet ska kunna underlåtas.

Vidare bör det finnas en möjlighet för nämnden att – på liknande sätt som gäller för kontrollmyndigheten enligt lagen om försvarsunderrättelseverksamhet – besluta att viss inhämtning genom signalspaning ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras. En förutsättning för ett sådant beslut bör vara att det vid en kontroll framkommer att inhämtningen inte är förenlig med lag eller annan författning eller med tillståndet till signalspaning. Även om tillståndsfrågan prövats av domstol, som då gjort bl.a. avvägningen mot integritetsintresset, kan det sedan tillstånd givits inträffa att förhållandena förändrats. Bl.a. av denna anledning bör en förutsättning för ett beslut av nämnden om att spaningen ska upphöra eller ett beslut om förstöring av inhämtade underrättelser vara att inhämtningen utgör ett intrång i den enskildes integritet som inte står i rimlig proportion till syftet med verksamheten. Säkerhets- och integritetsskyddsnämnden skulle i detta avseende få ett vidare mandat än kontrollmyndigheten i försvarsunderrättelseverksamheten.

Säkerhets- och integritetsskyddsnämndens beslut bör – liksom är fallet enligt gällande rätt beträffande nämndens beslut rörande kontroll av hemliga tvångsmedel m.m. – inte gå att överklaga.

Ytterligare överväganden kring en framtida tillsyn

Enligt min mening bör övervägas att slå ihop den kontrollmyndighet för signalspaning i försvarsunderrättelseverksamhet som beskrivs i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) med Säkerhets- och integritetsskyddsnämnden. För det talar resursbesparingar samt att den sammansättning och övriga organisation samt det regelsystem som föreslås gälla för kontrollmyndigheten på försvarsunderrättelseområdet är i det närmaste identiska med vad som redan i dag gäller för Säkerhets- och integritetsskyddsnämnden. För en sammanslagning talar också att det är samma skyddsintressen som ska bevakas av de båda organen. Mot det talar möjligen att den sammanslagna nämnden skulle få ett vidsträckt ansvarsområde och stor insyn i hemlig verksamhet.

Frågan om en sammanslagning av de båda myndigheterna rör emellertid mer än den tillsynsverksamhet över signalspaningen som här är aktuell och bör därmed beredas vidare i annat sammanhang.

7.11.2 Insynsrådet vid signalspaningsmyndigheten

Förslag: Insynsrådet vid signalspaningsmyndigheten ska ha insyn även i den signalspaning som utförs för polisens räkning.

Vid Försvarets radioanstalt ska enligt 11 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet finnas ett råd med uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten. Rådets ledamöter utses av regeringen för viss tid. Rådet ska rapportera sina iakttagelser till ledningen för Försvarets radioanstalt och, om rådet finner att det finns skäl för det, till Försvarets underrättelsenämnd.

Rådet bör ha insyn även i den signalspaningsverksamhet som bedrivs för polisens räkning. Rådet ska på samma sätt som inom försvarsunderrättelseverksamheten rapportera sina iakttagelser till ledningen för Försvarets radioanstalt. Rådet bör även, om det finner skäl för det, rapportera sina iakttagelser till kontrollmyndigheten, dvs. såvitt gäller polisens signalspaning till Säkerhets- och integritetsskyddsnämnden.

7.11.3 Rådigheten över signalbärarna

Bedömning: Rådigheten över signalbärarna bör anordnas på samma sätt för signalspaning som bedrivs för polisens räkning som för signalspaning i försvarsunderrättelseverksamheten.

Förslagna åtgärder inom försvarsunderrättelseverksamheten

Som redovisats ovan (avsnitt 7.6.3) föreslås i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) att ett tillstånd till signalspaning endast ska omfatta de signalbärare som behövs för att genomföra spaningen. Samtidigt föreslås i propositionen att rådigheten över signalbärarna endast ska tillkomma

kontrollmyndigheten, dvs. Försvarets underrättelsenämnd (eller den myndighet som ska ersätta nämnden).

Tanken är således att domstolen i sitt tillstånd ska ange de signalbärare som behövs för att genomföra uppdraget. Försvarets radioanstalt kommer därefter att kontakta Försvarets underrättelsenämnd som har att verkställa domstolens beslut, dvs. att ”koppla in” de signalbärare som Försvarets radioanstalt enligt tillståndet har rätt att använda. Nämnden har inte något eget handlingsutrymme och ska inte fatta något beslut. En sådan uppgift skulle riskera att komma i konflikt med nämndens tillsynsuppgifter. I stället ska nämnden endast vidta de praktiska åtgärder som behövs för att ge tillgång till de signalbärare som Försvarets radioanstalt anger och som följer av tillståndet.

Som redovisats ovan (avsnitt 7.7.6) ska det enligt förslaget i propositionen finnas möjlighet att i särskild ordning fatta beslut om signalspaning i brådskande fall. Försvarets underrättelsenämnd måste därmed, såvitt gäller nämndens uppgift att ha rådighet över signalbärarna, ha en beredskap att snabbt verkställa sådana åtgärder.

Överväganden angående rådigheten över signalbärarna

En utgångspunkt är att man kan knappast ha två myndigheter som förfogar över signalbärarna. Det skulle bli opraktiskt, svårt att hantera och kontrollera samt innebära ett resursslöseri.

Som jag redogjort för ovan finns enligt min mening skäl att överväga en sammanslagning av de båda tillsynsorgan som föreslås ha tillsynen över signalspaningen inom försvarsunderrättelseverksamheten respektive signalspaning som utförs för polisens räkning. Om det även fortsättningsvis ska vara olika kontrollorgan för försvarsunderrättelseverksamheten och polisens underrättelseverksamhet måste emellertid frågan om rådighet över signalbärarna lösas. Även om olika myndigheter – beroende på om signalspaningen sker inom ramen för försvarsunderrättelseverksamheten eller på uppdrag av Säkerhetspolisen eller den övriga polisen – kommer att ha tillsyn över verksamheten saknas skäl att låta två olika myndigheter utveckla den tekniska kompetens som krävs för att hantera signalbärarna. Uppgiften att ha rådighet över signabärarna innebär som nämnts ovan inte något handlingsutrymme för myndigheten i fråga och några beslut ska inte fattas. Det är heller ingen uppgift inom ramen för en tillsynsverksamhet. Därtill måste verksamheten med nödvändigheten ha en beredskap att verkställa

beslut om signalspaning dygnet runt. Mot denna bakgrund är det min uppfattning att för det fall statsmakterna beslutar att Försvarets underrättelsenämnd ska ha rådigheten över signalbärarna såvitt avser signal-spaning i försvarsunderrättelseverksamheten bör den nämnden ha samma uppgift vid signalspaning som utförs för polisens räkning.

Den lösning som föreslås i propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) kan emellertid ifrågasättas av principiella skäl. Förslaget innebär som nämnts ovan att ett statligt organ för tillsyn av signalspaning ska ges rådighet över signalbärarna. Förslaget medför att tillsynsorganet kommer att ta aktiv del i den verkställighet som det har till uppgift att utöva tillsyn över. Enligt min mening är detta inte en lämplig lösning. Ett tillsynsorgan bör inte ges i uppgift att ta del i den verksamhet som det har tillsyn över. En annan nackdel med modellen är att staten som sådan (genom tillsynsorganet) har total tillgång till de telekommunikationer som förs över Sveriges gräns. Det är en omständighet som kan ha betydelse vid en eventuell framtida prövning av om Sverige kan anses uppfylla kraven på förutsättningarna för ingrepp i rätten till skydd för privat- och familjeliv enligt artikel 8 i Europakonventionen.

På grund av det nu anförda anser jag att det i det fortsatta lagstiftningsarbetet bör övervägas om inte de aktuella teleoperatörerna i stället kan svara för att det till signalspaningsmyndigheten överförs endast sådan telekommunikationstrafik som omfattas av domstolens tillstånd. Det är en ordning som redan gäller i fråga om hemliga teletvångsmedel. Jag är medveten om att den frågan har övervägts i det hittillsvarande lagstiftningsarbetet (se den ovan nämnda propositionen s. 36 ff) och inser att den lösningen har nackdelar. Även den lösning som föreslås i propositionen är emellertid behäftad med sådana nackdelar att fortsätta överväganden är motiverade.

7.12 Särskilt om användning av underrättelsematerial som bevisning i rättegång

Förslag: Möjligheten för Säkerhetspolisen och den öppna polisen att använda underrättelsematerial som bevisning i rättegång bör ses över.

7.12.1 Bakgrund

Jag har i avsnitt 2.4 redogjort för vissa begränsningar i användningen av den information som polisen får tillgång till genom signalspaning. Begränsningen består i att ett offentliggörande av sådan information, t.ex. i samband med en rättegång, skulle kunna avslöja de metoder som Försvarets radioanstalt använder och den förmåga myndigheten har. Om metoder och förmåga avslöjas kan verksamheten komma att skadas på ett sådant sätt att en fortsatt verksamhet försvåras eller omöjliggörs. De underrättelser som Försvarets radioanstalt vidarebefordrar till polisen är mot denna bakgrund som huvudregel behäftade med ett förbud mot offentliggörande utan medgivande från Försvarets radioanstalt. Det bör framhållas att det numer har klargjorts att Försvarets radioanstalt inte biträder polisen under en förundersökning (se avsnitt 4.1.2).

Även om information från signalspaning således skulle innehålla avgörande bevisning för att en person har gjort sig skyldig till brott kan informationen normalt inte användas som bevisning i en rättegång, eftersom ingen information som används i det syftet kan hemlighållas, i vart fall inte för den tilltalade och dennes försvarare. I konsekvens härmed tvingas således polisen att avstå från lagföring i sådana fall.

Begränsningarna gör sig självklart gällande vid all form av signalspaning, dvs. både inom försvarsunderrättelseverksamheten och vid den signalspaning som utförs för polisens räkning. Eftersom en central uppgift för polisen är att lagföra kriminella individer för brott blir emellertid effekterna betydligt mer påtagliga för polisen än för myndigheterna inom försvarsunderrättelseverksamheten.

Problemet med att kunna använda information av väsentlig betydelse i polisarbetet utan att avslöja förhållanden som måste hållas hemliga är inte unikt för signalspaning. Samma hänsyn måste exempelvis tas när det gäller information från mänskliga källor, s.k. informatörer. Att öppet offentliggöra från vilken person informationen kommer och hur polisen kommit över informationen skulle både äventyra informatörens säkerhet och avslöja polisens arbetsmetoder. Därtill kommer att polisens möjligheter att fortsättningsvis värva nya informatörer allvarligt skulle försvåras om de tilltänkta informatörerna inte kan lita på att deras identitet och utsagor kan hemlighållas. Samma hänsyn måste tas i samband med att polisen får information från utländska samarbetspartners, dvs. myndigheter i andra länder. Sådan information lämnas ofta med

förbehåll om att den inte får föras vidare eller användas som bevisning i rättegång. Skälen till sådana förbehåll kan vara olika. Ofta handlar det om att skydda källor eller arbetsmetoder.

Vad gäller utländskt samarbete har en motsvarande problematik redan uppmärksammats i lagstiftningen. Exempelvis följer av 5 § lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar att om en svensk myndighet har fått uppgifter genom ett internationellt samarbete och det på grund av internationella överenskommelser gäller villkor som begränsar möjligheten att använda uppgifterna, ska myndigheten följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning. Regler i svensk rätt om skyldighet för svenska myndigheter att på grund av uppgifter som kommer till deras kännedom inleda förundersökning och väcka åtal gäller därmed inte i dessa fall (se prop. 2003/04:4 s. 30 för fler exempel på sådana bestämmelser i svensk rätt).

Redovisningen av förhållandena i andra länder (avsnitt 6.2) visar att problemet har uppmärksammats internationellt och att man i flera länder också har reglerat frågan i syfte att möjliggöra lagföring även i de fall det material som ligger till grund för ett åtal utgörs av information från signalspaning eller annan hemlig inhämtning av information. Det kan därtill tilläggas att det i Storbritannien helt nyligen på regeringens uppdrag har genomförts en utredning avseende dessa frågor (se Privy council review of intercept as evidence, Report to the Prime Minister and the Home Secretary, 30 januari 2008). De lösningar som valts skiftar mellan länderna. Syftet är emellertid detsamma, nämligen att kunna offentliggöra information som är av avgörande betydelse för polisen och domstolarna, utan att för den skull avslöja hemliga metoder och myndigheternas förmåga. I Sverige finns i dag, till skillnad från i flera andra länder, inte någon sådan möjlighet.

Vid en internationell jämförelse bör man dessutom ha i minnet att problemet i Sverige också är än mer komplicerat än i många andra länder. I Sverige finns, som beskrivits i avsnitt 6.1, varken någon civil utrikes underrättelsetjänst (utom Försvarets radioanstalt som står för inhämtningen genom signalspaning) eller någon civil säkerhetstjänst. Det material som delges den svenska säkerhetstjänsten, dvs. Säkerhetspolisen, delges därmed samtidigt Säkerhetspolisen i egenskap av polismyndighet. Säkerhetspolisens tudelade uppdrag har beskrivits i avsnitt 7.1.6. När de civila underrättelse- och säkerhetstjänsterna utomlands tar omhand informa-

tion från signalspaning för egen räkning – antingen genom egen inhämtning som huvudregeln är i Tyskland eller genom anlitande av en annan myndighet som huvudregeln är i Kanada (avsnitt 6.2) – har de möjlighet att överväga i vilken mån och på vilket sätt denna information ska delges exempelvis polisiära myndigheter. I Sverige har Försvarets radioanstalt att delge sina underrättelser direkt till Säkerhetspolisen eller den öppna polisen.

7.12.2 Överväganden kring behovet av en översyn

Frågan om att använda hemligt underrättelsematerial som en del av en förundersökning och även som bevisning i en rättegång har kommit att aktualiseras allt mer. Att bekämpa bl.a. terrorism och grov organiserad brottslighet har en hög prioritet i de flesta länder, så även i Sverige. Brottsbekämpningen på dessa områden kräver nya arbetsmetoder för att bli framgångsrik. Brottsligheten planeras i slutna grupperingar, ofta med kopplingar till utlandet. Traditionella polisiära arbetsmetoder räcker i dessa fall inte till. Polisen har därför under senare år getts tillgång till bl.a. användning av tvångsmedel i preventivt syfte och till hemlig rumsavlyssning. Bekämpningen kräver emellertid därtill att polisen använder andra dolda metoder såsom signalspaning och användning av informatörer.

Samma typ av fenomenen är därtill på en strategisk nivå också föremål för intresse inom försvarsunderrättelseverksamheten. Som framgått ovan är även den signalspaning som Försvarets radioanstalt bedriver på uppdrag av bl.a. regeringen och Försvarsmakten inriktad på områden som också är av intresse för den brottsbekämpande verksamheten. Regeringen har konstaterat att gränsen mellan inre/polisiär och yttre/militär säkerhet inte är lika klar som tidigare (se avsnitt 4.1.2). Information som rör kriminalitet hämtas således in på relativt bred front.

Att myndigheterna ägnar sig åt underrättelseinhämtning kring kriminella aktiviteter utan att ha för avsikt att i någon form använda denna information i syfte att utreda brott och att lagföra personer framstår enligt min mening som tveksamt. Att det huvudsakliga syftet med inhämtningen är kunskapshöjande och avser att skapa en beredskap är en sak. Om man i det arbetet finner avgörande bevisning bör emellertid – såsom är fallet i andra länder – möjligheten finnas att i någon form använda materialet. Därtill kan ju den situationen uppkomma att information som inte kan offentlig-

göras faktiskt talar till fördel för en misstänkt person, i värsta fall utan att åklagaren i en pågående förundersökning eller rättegång har kännedom om det. Att i ett sådant fall hemlighålla uppgifterna för försvararen och domstolen framstår självfallet som främmande.

Synen på säkerhetshotande verksamhet har förändrats och därmed måste även myndigheternas kunnande och tekniska förmåga utnyttjas på ett annat sätt än tidigare. Fokus för underrättelseinhämtningen har ändrats från den tid när försvarsunderrättelseverksamheten var inriktad mot yttre militära hot och när tyngdpunkten i Säkerhetspolisens verksamhet utgjordes av dess kontraspionage. En sådan ändring bör enligt min mening också få konsekvenser i rättskedjan. När statsmakternas intresse alltmer vänds mot kriminell verksamhet, t.ex. terrorism och grov organiserad brottslighet, bör också verktyg skapas för att möjliggöra lagföring av de individer som utövar den kriminella verksamheten. Det är bl.a. mot denna bakgrund som jag sett det som nödvändigt att föreslå att signalspaning ska kunna användas inte bara som en inhämtningsmetod inom underrättelseverksamheten utan också inom ramen för en förundersökning.

Samtidigt är jag väl medveten om att vissa metoder och viss förmåga hos polisen och samverkande myndigheter måste hållas hemliga för att kunna fungera effektivt. Det finns inte någon möjlighet för mig att inom ramen för detta utredningsuppdrag presentera en lösning på problematiken och därtill är frågan av betydelse även för annan typ av inhämtning än signalspaning. Det är emellertid min uppfattning att en översyn bör genomföras. Som nämnts finns förebilder internationellt.

7.12.3 Hemlighållande av metod och förmåga

Mitt förslag att under vissa förutsättningar kunna använda signalspaning inom ramen för förundersökningar har mötts med tvekan av bl.a. Försvarets radioanstalt. Tvekan har sin grund i risken för att myndighetens metoder och förmåga skulle komma att avslöjas. För att avhjälpa den problematiken skulle en bestämmelse av följande innehåll kunna införas i den föreslagna lagen:

> **X §** Underrättelser som inhämtats enligt denna lag genom signalspaning får tillföras en förundersökning rörande brott endast om det medges av signalspaningsmyndigheten.

Genom en sådan bestämmelse skulle Försvarets radioanstalt ges möjlighet att avgöra om det aktuella materialet kan offentliggöras eller inte.

Det är dessutom min bedömning att det material som Försvarets radioanstalt inhämtar med hjälp av signalspaning enligt den nu föreslagna lagstiftningen och den redan beslutade lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet bör kunna offentliggöras i större utsträckning än vad som hittills varit fallet. Verksamheten vid Försvarets radioanstalt var tills helt nyligen inte allmänt känd och var därtill inte reglerad. Det nu pågående lagstiftningsarbetet och den debatt som följt på det arbetet har ändrat på detta. Med den nya lagstiftningen är arbetsmetoderna offentligt reglerade och därtill allmänt kända, om än inte i varje teknisk detalj men i vart fall på en övergripande nivå. Av den redan gällande lagen om signalspaning i försvarsunderrättelseverksamheten framgår exempelvis vilken rätt Försvarets radioanstalt har att bedriva signalspaning i tråd och att spaningen utförs vid ett antal samverkanspunkter vid Sveriges gräns. I förarbetena finns beskrivningar av hur spaningen är tänkt att gå till när det gäller exempelvis användning av sökbegrepp. I den meningen är metoden därmed inte längre hemlig. Att Försvarets radioanstalt med polisen som uppdragsgivare – med stöd av den nu föreslagna lagen – har både den rättsliga befogenheten och den tekniska möjligheten att spana mot trådbunden trafik vid de s.k. samverkanspunkterna är därmed inte heller något som i sig behöver avslöja någon metod eller förmåga som inte redan är känd.

De uppdrag som Försvarets radioanstalt kommer att utföra för polisens räkning kan dessutom komma att redovisas på olika sätt. Beroende på polisens behov och Försvarets radioanstalts förmåga kan man tänka sig att redovisningarna sker genom allt från överlämnande av ljudupptagningar eller utskrifter till rapporter som varit föremål för omfattande bearbetning och analys. Genom valet av redovisningsform kan hänsyn tas till känslig information (jfr. avsnitt 7.9.1).

7.12.4 Överskottsinformation

Jag har i förslaget till lag om signalspaning för polisens behov avseende utrikes förhållanden föreslagit att domstolen i samband med tillståndsgivningen ska föreskriva vilken information, inklusive eventuell

överskottsinformation, som får överlämnas av Försvarets radioanstalt till polisen (se avsnitt 7.8.6 och kommentaren till 8 § första stycket i författningskommentaren, avsnitt 9.1). Bestämmelsen medför att eventuell överskottsinformation kommer att överlämnas endast i begränsad omfattning. Att eventuell överskottsinformation under vissa omständigheter får överlämnas till polisen har emellertid inte någon omedelbar betydelse för frågan hur eventuell överskottsinformation därefter får användas av polisen.

Den i avsnittet ovan beskrivna problematiken medför att bestämmelser om användning av överskottsinformation inte kan införas i den föreslagna lagen på motsvarande sätt som i rättegångsbalken och viss annan lagstiftning. Sådana bestämmelser skulle ha kunnat reglera dels i vilken mån information från signalspaning som inhämtats inom ramen för underrättelseverksamheten skulle få användas vid utredning av ett brott, dels i vilken mån information från signalspaning som framkommit vid utredningen av ett brott skulle få användas vid utredningen av ett annat brott.

Vad gäller den första frågan, dvs. hur material från signalspaning som inhämtats i underrättelsesyfte skulle få användas i en brottsutredning, hänvisas till resonemanget ovan angående en bredare översyn. Frågan har hittills varit oreglerad inom polisen. Polismetodutredningen har emellertid helt nyligen i betänkandet En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen (SOU 2009:01) presenterat ett förslag som i ett särskilt avseende reglerar frågan. Förslaget innebär att för det fall polisen i underrättelsesyfte inhämtar uppgifter om bl.a. telemeddelanden får dessa uppgifter användas i en brottsutredning endast om ett beslut om hemlig teleövervakning har fattats inom ramen för den brottsutredningen (betänkandet s. 181). Den metod som polisen i det fallet har att använda för att inhämta informationen är emellertid inte hemlig såvitt gäller tillvägagångssätt och förmåga. Bestämmelsen innehåller således inte någon avvägning mellan de motstående intressena, dvs. intresset av att å ena sidan hemlighålla myndigheternas metoder och förmåga och å andra sidan att kunna använda tillgängligt material för lagföring. Den valda lösningen är därmed inte heller användbar i samband med signalspaning.

I det andra fallet, dvs. i de få fall där signalspaning kommer att användas inom ramen för en förundersökning, saknar polisen i praktiken rätten att använda materialet på annat sätt än som medges av Försvarets radioanstalt. Det material som Försvarets radioanstalt i ett sådant fall skulle redovisa för polisen och som med myndighetens

medgivande skulle offentliggöras i samband med en rättegång torde därmed inte innehålla något annat än det som har betydelse för den aktuella domstolsprövningen. För det fall Försvarets radioanstalts medgivande ändå skulle öppna för att använda materialet även beträffande andra brott än det för vilket det inhämtats är det min uppfattning att bestämmelserna om överskottsinformation vid hemlig teleavlyssning i 27 kap. 23 a § rättegångsbalken bör tillämpas analogivis av polis och åklagare.

7.13 Ikraftträdande

I propositionen Förstärkt integritetsskydd vid signalspaning (prop. 2008/09:201) föreslås att de ändringar och tillägg i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet som framgår av propositionen ska träda i kraft den 1 december 2009. Samtidigt föreslås den föreslagna lagen om försvarsunderrättelsedomstol träda i kraft. Propositionen har i skrivande stund (juni 2009) ännu inte behandlats i riksdagen.

De förslag som jag presenterar i detta betänkande kan träda i kraft tidigast då de förslag som följer av den ovan nämnda propositionen träder i kraft. Det gäller såväl ändringarna och tilläggen i lagen om signalspaning i försvarsunderrättelseverksamhet som bestämmelserna kring den nya domstolen.

Även skyldigheten enligt lagen (2003:389) om elektronisk kommunikation för teleoperatörerna att överföra signaler måste ha trätt i kraft. Riksdagen har beslutat (bet. 2008/09:FöU11, rskr. 2008/09:245) att den skyldigheten ska träda i kraft den 1 december 2009.

Det är mot denna bakgrund inte möjligt att nu bedöma när de bestämmelser som föreslås i detta betänkande skulle kunna träda i kraft. För att undvika effektivitetsförluster i polisens verksamhet är det emellertid angeläget att bestämmelserna träder i kraft så snart som möjligt.

Vad gäller övergångsbestämmelser bör i likhet med vad som föreslås i den ovan nämnda propositionen avseende signalspaning i försvarsunderrättelseverksamheten gälla att verksamhet som vid ikraftträdandet bedrivs med stöd av tillstånd meddelade enligt äldre bestämmelser får bedrivas till dess att tiden för tillståndet löper ut. En sådan övergångsbestämmelse förutsätter emellertid att Försvarets radioanstalt vid ikraftträdandet alltjämt, enligt de bestämmelser som i skriv-

ande stund ännu gäller, har rätt att bedriva signalspaning för polisens räkning.

8 Ekonomiska konsekvenser av förslagen

Försvarets radioanstalt

Som har framgått av detta betänkande har Försvarets radioanstalt under flera årtionden biträtt polisen med signalspaning i etern. Förslagen i den delen innebär således inte annat än att en tidigare oreglerad verksamhet nu regleras och begränsas såvitt avser tillämpningsområdet. Några ökade kostnader med anledning av förslaget i den delen bedöms därmed inte föreligga.

Vad gäller signalspaning i tråd har Försvarets radioanstalts möjligheter att bedriva sådan verksamhet inom ramen för försvarsunderrättelseverksamheten redan beslutats av statsmakterna. De praktiska förutsättningarna för att bedriva sådan spaning, t.ex. investeringar i ny teknik m.m., genomförs därmed oberoende av förslagen i detta betänkande.

För Försvarets radioanstalts del kan mina förslag däremot komma att innebära att den information som myndigheten har att inhämta, bearbeta och analysera ökar. I vilken utsträckning detta kommer att innebära behov av ökade resurser är naturligtvis beroende på i vilken utsträckning polisen kommer att använda sig av den föreslagna lagstiftningen. Försvarets radioanstalt har mot den bakgrunden förklarat att de saknar möjlighet att nu uppskatta behovet av ökade resurser. Det finns dock enligt min bedömning inte anledning att anta att omfattningen under överblickbar tid kommer att bli större än att det ökade resursbehovet kommer att uppgå till högst 30 miljoner kr årligen. Sannolikt kommer beloppet enligt min bedömning att bli klart lägre än så.

Polisen

För Säkerhetspolisens och den övriga polisens del bedöms förslagen inte få några ekonomiska konsekvenser.

Domstolen

Vad gäller den föreslagna domstolsprövningen har regeringen såvitt avser signalspaning inom försvarsunderrättelseverksamheten föreslagit att en specialdomstol inrättas. Jag har i stället föreslagit att tillståndsprövningen bör genomföras i en allmän förvaltningsdomstol.

Om lagstiftaren skulle besluta att inrätta en specialdomstol är det min uppfattning att den domstolen också ska handlägga tillstånd till signalspaning enligt den nu förslagna lagen om signalspaning för polisens räkning. Eftersom den föreslagna specialdomstolen ännu inte påbörjat sin verksamhet (och i skrivande stund inte ens är beslutad) är det inte möjligt att inom ramen för denna utredning bedöma de extra kostnader som uppstår för det fall domstolen också ska handlägga ärenden på ansökan av polisen. Antalet ärenden som domstolen har att hantera kommer emellertid självfallet att öka jämfört med om domstolen enbart skulle hantera ärenden inom försvarsunderrättelseverksamheten. Det kan tilläggas att regeringen har för avsikt att tillkalla en särskild utredare med uppdraget att förbereda inrättandet av specialdomstolen (prop. 2007/08:201 s. 108).

För det fall tillståndsfrågorna skulle komma att avgöras av en allmän förvaltningsdomstol uppstår ökade kostnader vid den domstolen. En förutsättning för en sådan lösning är emellertid att den domstolen kommer att hantera alla ärenden om tillstånd till signalspaning, dvs. även tillstånd till signalspaning inom försvarsunderrättelseverksamheten. Jag saknar möjlighet att inom ramen för detta utredningsuppdrag bedöma kostnaden för en sådan reform eftersom jag saknar kännedom om vilken ärendevolym som då blir aktuell. De ärenden som skulle hänföra sig till signalspaning för polisens räkning och som jag kan överblicka torde endast utgöra en mindre del av de ärenden som den domstolen skulle ha att handlägga.

Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden föreslås utöva tillsyn över polisens signalspaning. För den uppgiften kommer nämnden att behöva ytterligare resurser motsvarande fyra årsarbetskrafter, vilket med lokal-, säkerhetsskydds- och andra kringkostnader kan beräknas motsvara en årlig kostnad om 5,5 miljoner kr.

Kontrollmyndigheten i försvarsunderrättelseverksamheten

Den kontrollmyndighet som ska utöva tillsyn över den signalspaning i försvarsunderrättelseverksamheten, en ombildning av den nuvarande Försvarsunderrättelsenämnden, ska enligt regeringens förslag i propositionen Förstärkt integritetsskydd vid signalspaning (2008/09:201) ha rådigheten över de s.k. signalbärarna. Regeringen har framhållit att åtgärderna kan behöva kunna vidtas även utanför ordinarie arbetstid. Kostnader för utrustning för att utföra det uppdraget har beaktats av regeringen i samband med de föreslagna ändringarna (prop. s. 108).

Det är min bedömning att konsekvenserna för kontrollmyndigheten när det gäller att utföra detta uppdrag även beträffande den signalspaning som föreslås för polisen räkning (se avsnitt 7.11.3) blir små, men att en ökning av antalet ärenden naturligtvis blir fallet. Konsekvenserna för myndigheten vad gäller den utrustning som behövs och den beredskap som krävs följer emellertid redan av regeringens förslag beträffande signalspaning i försvarsunderrättelseverksamheten.

9 Författningskommentar

9.1 Förslaget till lag om signalspaning för polisens behov avseende utrikes förhållanden

1 §

Polisen får använda signalspaning i syfte att avslöja och utreda eller förhindra brott för vilket är föreskrivet fängelse två år eller däröver.

Säkerhetspolisen får använda sådan spaning även i annat fall än som avses i första stycket, om det behövs för att motverka

1. underrättelseverksamhet som kan antas bedrivas av främmande makt eller av organisation som huvudsakligen finns utomlands, om verksamheten är riktad mot Sverige eller svenska intressen eller på annat sätt berör Sverige,
2. annat allvarligt hot mot rikets säkerhet,
3. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
4. internationell terrorism, eller
5. annan grov organiserad brottslighet.

Signalspaning i tråd får ske endast i enlighet med vad som anges i 4–6 §§.

Paragrafen reglerar de grundläggande förutsättningarna för att polisen ska få bedriva signalspaning.

Med signalspaning avses detsamma som i 1 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, dvs. inhämtning av signaler i elektronisk form (se prop. 2006/07:63 s. 136 f).

En första förutsättning för signalspaning är att det sker i syfte att avslöja, utreda eller förhindra brott. Bestämmelsen gör således ingen skillnad på om spaningen utförs i underrättelsesyfte eller inom ramen för en förundersökning. Det är emellertid inte misstanke om vilka brott som helst som kan ge möjlighet att använda signalspaning. Det krävs att det är brott av en viss svårighetsgrad. Uteslutet är att använda signalspaning vid misstanke om sådana brott där endast böter ingår i straffskalan. Detsamma gäller även

brott för vilka fängelse ingår i straffskalan, om den maximala fängelsepåföljden i straffskalan understiger två år. I paragrafens *första stycke* anges därför att signalspaning får användas bara för att avslöja, utreda eller förhindra brott som är så allvarliga att det för brottet är föreskrivet fängelse två år eller däröver. Bestämmelsen har behandlats i avsnitt 7.4.1.

Av *andra stycket* framgår att Säkerhetspolisen får använda signalspaning i vissa angivna fall, trots att förutsättningarna i första stycket inte är uppfyllda. De uppräknade fallen är uttömmande. Det rör sig om två fall av allvarliga hot mot rikets säkerhet samt tre fall som inte är kopplade till skyddet av den säkerheten. Signalspaningen får bara användas för att motverka de uppräknade verksamheterna. Bestämmelsen har behandlats i avsnitt 7.4.2.

För signalspaning i etern är de i 1 § angivna förutsättningarna uttömmande. Av *tredje stycket* följer att det i lagen finns ytterligare begränsningar när det gäller förutsättningarna för såväl den öppna polisen som Säkerhetspolisen att signalspana i tråd. Dessa begränsningar följer av 4–6 §§.

Mot denna bakgrund utgör i praktiken bestämmelserna i första stycket de grundläggande förutsättningar under vilka den öppna polisen kan använda signalspaning i etern och andra stycket de grundläggande förutsättningar under vilka Säkerhetspolisen kan använda signalspaning i etern.

2 §

> Signalspaning enligt denna lag får inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen av meddelandets innehåll förstöras så snart det står klart att sådana signaler har inhämtats.
>
> Signalspaningen får ske endast om syftet med spaningen väger klart tyngre än det integritetsintrång som spaningen kan medföra för enskilda och det syftet inte kan tillgodoses på ett mindre ingripande sätt.

Syftet med lagen är att reglera signalspaning för polisens behov avseende utrikes förhållanden. Mot den bakgrunden har i *första stycket* tagits in en bestämmelse om att signalspaning enligt lagen inte får avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. För att signalspaning ska var tillåten

enligt denna lag krävs således att antingen avsändaren eller mottagaren av ett meddelande befinner sig utomlands.

Eftersom det inte är möjligt att med nuvarande teknik fullt ut avskilja sådan trafik kompletteras förbudet med en skyldighet att förstöra upptagning eller uppteckning av inhemsk trafik så snart det står klart att signalspaningen har avsett sådan trafik.

Dessa frågor har behandlats i avsnitt 7.4.4.

Även om de i 1 § angivna förutsättningarna för att få använda signalspaning är uppfyllda är det inte tillräckligt för att arbetsmetoden ska få användas i det enskilda fallet. I *andra stycket* finns nämligen en betydande begränsning i rätten att använda signalspaning. Bestämmelsen innebär att signalspaning får ske endast om syftet med spaningen väger klart tyngre än det integritetsintrång som spaningen kan medföra för enskilda och det syftet inte kan tillgodoses på ett mindre ingripande sätt. Bestämmelsen är uppställd till skydd för den personliga integriteten. Den innebär att det ska göras två prövningar i varje enskilt fall där frågan om signalspaning ska få ske prövas. Den ena prövningen avser att undersöka om syftet med spaningen väger *klart* tyngre än integritetsintrånget. Med ordet ”klart” avses i lagtexten att markera att det inte får vara någon tvekan om att syftet väger tyngre. Vid minsta tvekan kan rekvisitet ”väger klart tyngre” inte anses vara uppfyllt. I bedömningen av om syftet väger klart tyngre får bl.a. omfattningen och allvaret i det hot som spaningen ska avse betydelse. Också frågan om hotet är akut eller mera avlägset kan vara av vikt vid den bedömningen. Omfattningen av befarat integritetsintrång är en faktor som också bör beaktas i sammanhanget.

Bedömningen bör normalt ge vid handen att signalspaning i etern för den öppna polisens räkning inte får avse annat än allvarlig brottslighet, främst grov organiserad brottslighet med gränsöverskridande inslag.

Den andra prövningen ska visa att syftet med signalspaningen inte kan tillgodoses på något annat sätt, t.ex. genom att anlita personer som källor, genom annan typ av spaning eller underrättelseinhämtning av annat slag. Den bedömningen torde vad gäller den vanliga polisen i de allra flesta fall utesluta signalspaning som en inhämtningsmetod, eftersom traditionella arbetsmetoder och användningen av befintliga straffprocessuella tvångsmedel normalt måste anses tillgodose polisens behov.

Vad gäller signalspaning inom ramen för en brottsutredning bör klargöras att eftersom signalspaning leder till ett bredare integritetsintrång än hemlig teleavlyssning, måste därtill signalspaning anses mer

ingripande än hemlig teleavlyssning. Bestämmelsen i 2 § andra stycket får därför anses innebära att signalspaning inte får tillgripas om syftet med spaningen i stället kan tillgodoses genom hemlig teleavlyssning. Det gäller också i de fall då hemlig teleavlyssning kan åstadkommas mot en teleadress utomlands med hjälp av myndigheterna i det land där teleadressen finns (se bestämmelserna om rättslig hjälp i lagen [2000:562] om internationell rättslig hjälp i brottmål). Detta innebär att signalspaning för polisens räkning inte får förekomma om en hemlig teleavlyssning skulle vara möjlig att verkställa i Sverige eller om sådan avlyssning skulle vara möjlig att verkställa utomlands med stöd av internationella överenskommelser.

Frågan om proportionalitetsbedömningen har behandlats i avsnitt 7.4.3.

3 §

> Signalspaning ska för polisens räkning utföras av den signalspaningsmyndighet som avses i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
>
> Den signalspaningsmyndighet som avses i första stycket får även i övrigt biträda polisen med tekniskt stöd.
>
> Om det är nödvändigt för signalspaning enligt denna lag får signaler i elektronisk form inhämtas även i de syften som anges i 1 § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet. Utan hinder av vad som föreskrivs i 9 § första stycket denna lag ansöker signalspaningsmyndigheten om tillstånd för sådan signalspaning.

Av *första stycket* följer att det är samma myndighet som enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska bedriva signalspaningen i försvarsunderrättelseverksamheten som ska bedriva signalspaning för polisens räkning enligt denna lag, dvs. Försvarets radioanstalt. Polisen ska således inte i egen regi bedriva signalspaning enligt denna lag. Frågan har behandlats i avsnitt 7.8.

Av *andra stycket* följer att signalspaningsmyndigheten även i övrigt får biträda polisen med tekniskt stöd. Här avses exempelvis stöd i form av kryptoforcering. Bestämmelsen utgör ett förtydligande i förhållande till vad som i praktiken redan gäller och som har sin grund i allmänna förvaltningsrättsliga principer om samverkan myndigheter emellan.

Signalspaningsmyndigheten får enligt *tredje stycket*, om det är nödvändigt för att bedriva signalspaning enligt denna lag, inhämta signaler i elektronisk form i de syften som anges i 1 § tredje stycket

lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Av den bestämmelsen följer att signalspaningsmyndigheten får bedriva viss inhämtning med syftet att tillgodose myndighetens egna behov av teknik- och kompetensutveckling. Sådan inhämtning är en förutsättning för att signalspaningsverksamheten ska kunna bedrivas. Av 1 § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet följer att signalspaningsmyndigheten får bedriva sådan inhämtning 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 verksamhet enligt den lagen.

Genom att det i bestämmelsen hänvisas till bestämmelsen i lagen om signalspaning i försvarsunderrättelseverksamhet klargörs att det ska vara fråga om samma förutsättningar i de båda lagarna.

För sådan inhämtning gäller i tillämpliga delar de generella förutsättningar för signalspaning som i övrigt följer av denna lag, dvs. 2, 7, 8 och 9 §§. Tillstånd ska i dessa fall emellertid begäras av signalspaningsmyndigheten och inte av polisen.

Hänvisningen till lagen om signalspaning i försvarsunderrättelseverksamhet avser lagen i dess föreslagna lydelse i prop. 2008/09:201 (se bilaga 2).

4 §

> Inhämtning av signaler i tråd ska ske automatiserat. För sådan inhämtning gäller i övrigt vad som föreskrivs i 2 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Paragrafen innehåller grundläggande bestämmelser för signalspaning i tråd.

Av paragrafen följer att signalspaning i tråd alltid ska ske automatiserat. Skälen härför har behandlats i avsnitt 7.6.1.

Av paragrafen följer vidare, genom en hänvisning till 2 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, att inhämtning av signaler i tråd endast får avse signaler som förs över Sveriges gräns av en operatör. Med operatör avses detsamma som i 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation. Genom hänvisningen klargörs att signalspaning i tråd enligt denna lag ska ske

under samma förutsättningar som enligt lagen om signalspaning i försvarsunderrättelseverksamhet.

Hänvisningen till lagen om signalspaning i försvarsunderrättelseverksamhet avser lagen i dess nuvarande lydelse.

5 §

> Signalspaning i tråd får ske mot den som är skäligen misstänkt för brott om åtgärden är av synnerlig vikt för utredningen. För brottet får inte vara föreskrivet lindrigare straff än fängelse i två år. Spaningen får dock även avse dels försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff, dels annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.
>
> Signalspaning i tråd får också ske, om det finns särskild anledning att anta att en person kommer att utöva sådan brottslig verksamhet som avses i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Paragrafen reglerar de närmare förutsättningarna för polisens signalspaning i tråd. De förutsättningar som anges i paragrafen är identiska med de förutsättningar som gäller för polisens rätt att använda hemlig teleavlyssning. Polisen ska alltså kunna bedriva signalspaning i tråd bara i sådana fall då polisen i stället skulle kunna ha bedrivit hemlig teleavlyssning. Liksom vid hemlig teleavlyssning rör det sig alltså enbart om fall där misstanke om allvarlig brottslighet föreligger. Frågan har behandlats i avsnitt 7.5.2.

Bestämmelserna innebär i praktiken att tillstånd till signalspaning bara kan ges om polisen skulle kunna ha fått tillstånd till hemlig teleavlyssning i samma fall och mot samma mål. Det ska alltså inte vara möjligt att kringgå reglerna om hemlig teleavlyssning genom att i stället använda signalspaning. Värdet av bestämmelserna i denna paragraf ligger i stället i att det inte sällan är praktiskt omöjligt för svensk polis att använda hemlig teleavlyssning även om förutsättningarna för att erhålla tillstånd till det är uppfyllda. Så kan exempelvis vara fallet om avlyssningen behöver sättas in mot en person som befinner sig utomlands och någon medverkan från det landets myndigheter inte kan påräknas för att få avlyssningen till stånd. I så fall kan signalspaning mot personen i fråga vara ett lämpligt förfaringssätt.

I paragrafens *första stycke* behandlas fallet att förundersökning pågår mot den misstänkte. I *andra stycket* behandlas möjligheten att

bedriva signalspaningen i preventivt syfte, dvs. i situationer där det finns särskild anledning att anta att en person kommer att utöva viss allvarlig brottlig verksamhet. I båda styckena motsvarar regleringen vad som gäller vid hemlig teleavlyssning.

Det bör erinras om att de väsentliga begränsningar i rätten att använda signalspaning som följer av 2 § andra stycket, dvs. att syftet med spaningen ska väga klart tyngre än det integritetsintrång som spaningen kan medföra för enskilda och syftet ska inte kunna tillgodoses på något annat sätt, gäller även vid signalspaning i tråd. Begränsningarna ska beaktas av domstolen vid tillståndsprövningen (se kommentaren till 2 §).

Att bestämmelserna om hemlig teleavlyssning inte ska kunna kringgås medför också att de andra regelverk som kan komma att aktualiseras i samband med en hemlig teleavlyssning måste beaktas. Bestämmelserna i lagen (2000:562) om internationell rättslig hjälp i brottmål berör bl.a. hemlig teleavlyssning, såsom dessa frågor har reglerats i 2000-års EU-konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (se närmare prop. 2004/05.144). Beträffande andra länder än konventionsstaterna ska naturligtvis eventuella folkrättsliga principer och förpliktelser kring brottsutredande verksamhet beaktas.

Att Säkerhetspolisen har rätt ett bedriva signalspaning i tråd även under andra förutsättningar än vad som följer av den nu behandlade paragrafen följer av 6 § nedan som behandlar signalspaning i tråd i underrättelsesyfte.

De begränsningar i fråga om signalspaning i tråd som följer av 5 § anger emellertid uttömmande förutsättningarna för den öppna polisen och för Säkerhetspolisen såvitt gäller spaning i tråd i syfte att utreda brott under en pågående förundersökning.

6 §

> Signalspaning i tråd får ske för att inhämta underrättelser som avses i 1 § andra stycket 1–4. Om sådan brottslighet som avses i 1 § andra stycket 5 utgör ett hot mot det demokratiska systemet i Sverige eller mot rättssystemet här, får signalspaning i tråd ske för att inhämta underrättelser som behövs för att motverka brottsligheten.

Paragrafen reglerar Säkerhetspolisens rätt att använda signalspaning i tråd för att inhämta underrättelser om säkerhetshotande verksamhet.

Befogenheten gäller således utöver de befogenheter för Säkerhetspolisen som framgår av 5 §.

Paragrafen reglerar säkerhetstjänstens rätt att använda signalspaning i tråd för att inhämta underrättelser om säkerhetshotande verksamhet. Det är alltså fråga om att avvärja hot av allvarlig karaktär. Att signalspaningen ska ske i underrättelsesyfte innebär att det inte får komma i fråga att tillämpa bestämmelsen i syfte att skaffa fram bevis inom ramen för en förundersökning. För signalspaning i tråd i ett sådant syfte hänvisas till de begränsade befogenheter som framgår av 5 §.

Säkerhetshoten ska vara av det slag som nämns i 1 § andra stycket, dvs. samma förutsättningar som gäller för Säkerhetspolisens signalspaning i etern. Signalspaning i tråd får emellertid sättas in med anledning av grov organiserad brottslighet bara om brottsligheten utgör ett hot mot det demokratiska systemet i Sverige eller mot rättssystemet här. Det innebär att signalspaning i tråd mot grov organiserad brottslighet kommer att kunna användas endast i de undantagsfall då den brottsligheten är systemhotande. Det kan t.ex. vara fallet om grovt kriminella gäng hotar domare med våld mot deras familjer om inte domarna frikänner åtalade gängmedlemmar.

Frågan har behandlats i avsnitt 7.5.3.

7 §

För signalspaning i tråd och annan automatiserad inhämtning gäller i övrigt 3 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Utan hinder av vad som föreskrivs i första stycket får ett sökbegrepp vara direkt hänförligt till en fysisk person, om signalspaningen sker med stöd av 5 § eller om det annars finns särskilda skäl.

Av *första stycket* framgår, genom en hänvisning till 3 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, att inhämtning av signaler som sker automatiserat endast får avse signaler som identifierats genom sökbegrepp. Bestämmelsen träffar därmed all inhämtning i tråd och den signalspaning i etern som sker automatiserat. Vidare innebär hänvisningen att sökbegreppen ska utformas och användas på ett sätt som är förenligt med respekten för den personliga integriteten.

Av *andra stycket* följer att förutsättningarna för att använda sökbegrepp som är hänförliga till en viss fysisk person skiljer sig åt mellan lagen om signalspaning i försvarsunderrättelseverksamhet och denna lag. För signalspaning enligt denna lag gäller att sådana sökbegrepp får användas dels om spaningen sker med stöd av 5 § (dvs. under samma

förutsättningar som gäller för hemlig teleavlyssning), dels om det annars finns särskilda skäl.

Frågan om användning av sökbegrepp har behandlats i avsnitt 7.6.2.

Hänvisningen till lagen om signalspaning i försvarsunderrättelseverksamhet avser lagen i dess föreslagna lydelse i prop. 2008/09:201 (se bilaga 2).

8 §

> Signalspaning kräver tillstånd. Sådant tillstånd lämnas av Länsrätten i Stockholms län. Tillstånd till signalspaning i tråd ska begränsas till sådana signalbärare som behövs för att uppnå syftet med spaningen. Av domstolens tillstånd ska vidare framgå vilka uppgifter från signalspaningen som får lämnas till polisen.
>
> Tillstånd får ges för högst tre månader. Domstolen får förlänga tiden med högst tre månader i taget.
>
> Vid handläggningen gäller vad som föreskrivs i 27 kap. 26–30 §§ rättegångsbalken.

I *första stycket* slås fast att signalspaning alltid kräver tillstånd av domstol. Tillståndsfrågan avgörs av Länsrätten i Stockholms län. Frågan har behandlats i avsnitt 7.7.

Domstolen ska begränsa tillstånden till sådana signalbärare som behövs för att uppnå syftet med spaningen. Frågan om signalbärare har behandlats i avsnitt 7.6.3.

Av första stycket följer också att domstolen, när den meddelar ett tillstånd till signalspaning, i tillståndsbeslutet ska ange i vilken utsträckning det som inhämtats genom signalspaningen får av Försvarets radioanstalt överlämnas till polisen. Avsikten är att begränsa polisens rätt att få del av det som inhämtats till sådan information som rör den fråga som föranlett tillståndet. Om exempelvis det beviljade tillståndet avsett att Försvarets radioanstalt för polisens räkning i en viss signalbärare ska spana efter information som rör ett visst företags handel med ämnen som kan användas för tillverkning av massförstörelsevapen, bör i domstolens tillstånd anges att endast sådan information som rör detta företags handel får överlämnas till polisen. Dock bör domstolen, om inga särskilda skäl talar emot det, också kunna ange att överskottsinformation från signalspaningen under vissa förutsättningar (se nedan) ska kunna överlämnas till polisen.

Vid tillämpning av bestämmelsen kommer kravet på precisering av i vilken utsträckning som Försvarets radioanstalt får överlämna information till polisen att bli starkare vid sådana tillstånd som domstolen

ger med stöd av 5 §. I dessa fall bör domstolens tillstånd innehålla att endast sådan information som rör den misstänkte eller den misstanke som legat till grund för domstolens beslut bör – jämte överskottsinformation – få överlämnas till polisen. Vad gäller överskottsinformation bör emellertid domstolen ange att sådan får överlämnas med samma begränsningar som gäller för polisens användning av överskottsinformation i samband med hemlig teleavlyssning (se 27 kap. 23 a § rättegångsbalken). Härigenom begränsas polisens rätt att få del av överskottsinformation kraftigt och får samma omfattning som vid hemlig teleavlyssning. Om tillståndet ges med stöd av 6 § kan däremot en vidare ram för överlämnandet föreskrivas av domstolen. I båda fallen måste dock utgångspunkten vara de syften för vilka tillståndet sökts, i den utsträckning som domstolen bifallit ansökan.

I vissa fall kan domstolen ha anledning att ytterligare begränsa polisens rätt att få del av information. Det kan t.ex. vid tillstånd enligt 5 § vara fallet om den information som polisen får efter en sådan begränsning är tillräcklig för att polisen med hjälp av den informationen ska kunna utreda brottet vidare genom användning av de vanliga tvångsmedlen i rättegångsbalken.

Ges tillståndet med stöd av 6 § kan också domstolen ha anledning att ge polisen en vidare rätt att ta del av överskottsinformation. Utöver de fall som motsvarar vad som gäller vid hemlig teleavlyssning bör även sådan överskottsinformation som rör frågor rörande rikets säkerhet av det slag som anges i 6 § kunna få lämnas till Säkerhetspolisen, om inte något särskilt skäl talar emot det i det enskilda tillståndsfallet.

Vad som nu har anförts har främst avsett signalspaning i tråd. Bestämmelsen är emellertid generell och gäller därmed även för spaning i etern. Det anförda kan därför även tillämpas på motsvarande sätt vid tillstånd till eterspaning.

Frågan om vilken information signalspaningsmyndigheten ska överlämna har behandlats i avsnitt 7.8.6.

Av *andra stycket* följer att tillståndstiden får vara högst tre månader i taget. Vid varje omprövningstillfälle ska en granskning ske av de resultat som uppnåtts i syfte att bedöma om fortsatt tillstånd framstår som meningsfullt. Prövningen ska göras bl.a. mot bakgrund av bestämmelserna i 2 § andra stycket.

Av hänvisningarna till rättegångsbalken i *tredje stycket* följer att offentliga ombud ska bevaka enskildas integritetsintressen i ärenden om signalspaning hos domstolen. Vad som i de angivna paragraferna i

rättegångsbalken stadgas om offentliga ombud ska gälla även vid tillståndsprövningen enligt denna lag.

Av 22 a § förvaltningslagen (1986:223) följer att länsrättens beslut kan överklagas till kammarrätten.

9 §

> Ansökan om tillstånd görs av polisen med biträde av signalspaningsmyndigheten. Ansökan ska innehålla uppgift om grunderna för ansökan. Beträffande sådan ansökan gäller i övrigt vad som anges i 4 a § 2–5 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
>
> Domstolen får förena ett tillstånd med de villkor som behövs för att begränsa intrånget i enskildas personliga integritet.
>
> Om det för fullgörandet av ett inhämtningsuppdrag för vilket tillstånd redan givits uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp, ska särskilt tillstånd sökas. Ett sådant tillstånd ska ha samma varaktighet som tillståndet för det inhämtningsuppdrag inom vilket tillgång till signalerna behövs eller sökbegreppen är avsedda att användas.

Av första stycket framgår att ansökan om tillstånd ska göras av polisen, dvs. i praktiken av antingen Säkerhetspolisen eller Rikskriminalpolisen. Signalspaningsmyndigheten ska biträda polisen i samband med ansökan i de delar det behövs, framför allt vad gäller de sökbegrepp som behövs vid signalspaningen och de signalbärare som är nödvändiga att få tillgång till för att utföra uppdraget.

Som framgår av 3 § tredje stycket är bestämmelsen försedd med ett undantag. I de fall syftet med signalspaningen är begränsat till signalspaningsmyndighetens eget behov av teknik- och kompetensutveckling är det signalspaningsmyndigheten som själv står för ansökan.

Av 1 a § andra stycket förundersökningskungörelsen (1947:948) följer att inom ramen för en förundersökning har förundersökningsledaren ansvar för förundersökningen i dess helhet. För det fall en åklagare är förundersökningsledare i en utredning där tillstånd till signalspaning begärs måste därmed ansökan om tillstånd göras med åklagarens godkännande.

Genom hänvisningen till 4 a § 2–5 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet klargörs att ansökan till domstolen ska ha innehålla detsamma som vid en ansökan enligt den lagen. Bestämmelsen har behandlats i avsnitt 7.7.7.

Av *andra stycket* framgår att domstolen får förena ett tillstånd med sådana villkor som behövs för att begränsa intrånget i enskil-

das personliga integritet. Av bestämmelserna i lagen framgår redan att domstolen dels ska godkänna de sökbegrepp som ska få användas, dels de signalbärare som signalspaningsmyndigheten ska få tillgång till. Domstolen kan med stöd av bestämmelsen i andra stycket förena tillståndet också med andra villkor för att begränsa intrånget i enskildas personliga integritet. Vilka villkor som aktualiseras är beroende av omständigheterna i det enskilda ärendet. Bestämmelsen motsvarar 5 a § första stycket 5 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet i dess föreslagna lydelse i prop. 2008/09:201, se bilaga 2.

När väl domstolen har beviljat tillstånd till signalspaning kan inom ramen för signalspaningsuppdraget uppkomma behov av ändringar i tillståndet, framför allt såvitt gäller vilka sökbegrepp som behöver användas och vilka signalbärare som signalspaningsmyndigheten behöver ha tillgång till. Av *tredje stycket* följer en möjlighet att göra en särskild ansökan om detta. Ansökan är inte fristående utan ska ha en anknytning till en redan beviljad ansökan. För en sådan ansökan och prövningen av den gäller samma regler som för den ursprungliga ansökan. Varaktigheten är knuten till det underliggande tillståndets varaktighet. Bestämmelsen motsvarar 5 a § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet i dess föreslagna lydelse i prop. 2008/09:201, se bilaga 2.

Hänvisningen till lagen om signalspaning i försvarsunderrättelseverksamhet avser lagen i dess föreslagna lydelse i prop. 2008/09:201 (se bilaga 2).

10 §

Om det kan befaras att inhämtande av domstolens tillstånd skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för något av de i 1, 5 och 6 §§ angivna ändamålen, får tillstånd till signalspaningen ges av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver.

Har tillstånd lämnats enligt första stycket ska åtgärden genast anmälas skriftligen till domstolen. I anmälan ska skälen för åtgärden anges. Domstolen ska då skyndsamt pröva ärendet och, om den finner att det inte finns skäl för åtgärden, upphäva beslutet.

Om ett beslut enligt första stycket har upphört att gälla innan rätten har prövat ett ärende enligt andra stycket, ska åtgärden anmälas till Säkerhets- och integritetsskyddsnämnden.

I paragrafen regleras den situationen att ett behov av signalspaning uppstår så brådskande att domstolens tillstånd inte kan inväntas utan att syftet med spaningen går förlorat. Bestämmelsen motsvarar 5 b § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet i dess föreslagna lydelse i prop. 2008/09:201, se bilaga 2.

Av *första stycket* framgår att signalspaning utan domstolens tillstånd är möjlig endast om inhämtande av ett tillstånd skulle innebära en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för något av de ändamål för vilka signalspaning enligt denna lag får användas. Att dröjsmålet ska vara av väsentlig betydelse innebär att det ska röra sig om situationer där själva syftet med spaningen riskerar att gå förlorat om domstolens tillstånd skulle avvaktas.

En ansökan om signalspaning i en sådan situation ska göras av polisen till signalspaningsmyndigheten. Rätten att besluta om signalspaning i ett sådant fall tillkommer endast en av regeringen särskilt utsedd befattningshavare vid signalspaningsmyndigheten.

Enligt *andra stycket* ska en sådan åtgärd omedelbart anmälas till domstolen. Härmed avses att ett beslut om att tillåta signalspaning och anmälan härom till domstolen ska göras i ett sammanhang. Skyldigheten bör lämpligen åligga den befattningshavare vid signalspaningsmyndigheten som av regeringen har medgetts rätt att fatta besluten och denne ska i anmälan till domstolen ange skälen för åtgärden.

Domstolen ska skyndsamt pröva ärendet och ska, om den finner att det inte har funnits skäl för åtgärden, upphäva beslutet. I sådant fall ska verksamheten naturligtvis genast avbrytas.

Möjligheten att besluta om signalspaning i brådskande fall gäller såväl ordinarie tillstånd som kompletterande tillstånd för tillgång till andra signalbärare eller användning av andra sökbegrepp än sådan som omfattas av ordinarie tillstånd.

Den situationen kan uppstå att signalspaning inleds på grund av ett beslut i brådskande fall, men att spaningen avbryts innan domstolen har hunnit pröva ärendet. Någon prövning av om de åtgärder som vidtagits varit lagligt grundade kommer i de fallen inte att göras av annan än den befattningshavare vid signalspaningsmyndigheten som fattade beslutet att inleda signalspaning. För att upprätthålla tillförlitligheten i systemet ska enligt *tredje stycket* åtgärden i sådana fall därför anmälas till Säkerhets- och integritetsskyddsnämnden. Skyldigheten att göra en sådan anmälan bör lämpligen tillkomma den befattningshavare vid signalspaningsmyndigheten som av regeringen givits rätt att fatta beslut om signalspaning i brådskande fall.

Frågor om beslut i brådskande fall har behandlats i avsnitt 7.7.6.

11 §

Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn över signalspaning som sker enligt denna lag.

Nämnden är skyldig att på begäran av en enskild kontrollera om hans eller hennes kommunikation har inhämtats i samband med signalspaning enligt denna lag eller om uppgifter om den enskilde har inhämtats genom den signalspaningen och lämnats till polisen och bevaras hos polisen eller om polisen i övrigt bevarar sådana uppgifter om den enskilde som inhämtats genom signalspaning. Kontrollen ska särskilt inriktas på om förfarandet skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen har utförts.

För tillsynen gäller i övrigt vad som föreskrivs i 2, 4 och 6 §§ lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Nämnden får besluta att viss inhämtning genom signalspaning ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med lag eller författning eller med tillstånd enligt denna lag eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten.

I denna paragraf regleras tillsynen över polisens signalspaningsverksamhet. Frågorna har behandlats i avsnitt 7.11.1.

Liksom när det gäller polisens användning av hemliga tvångsmedel och andra hemliga arbetsmetoder, t.ex. kvalificerade skyddsidentiteter, ska enligt *första stycket* tillsynen över signalspaningsverksamheten handhas av Säkerhets- och integritetsskyddsnämnden.

Av *andra stycket* följer att nämnden, liksom när det gäller polisens användning av hemliga tvångsmedel, på begäran av en enskild ska kontrollera om denne har varit utsatt för signalspaning och om det har skett lagenligt. Nämnden ska också på samma sätt som när det gäller hemliga tvångsmedel underrätta den enskilde om att kontrollen har skett. Säkerhets- och integritetsskyddsnämnden brukar därvid också ange om det har upptäckts något olagligt.

I *tredje stycket* hänvisas till vissa bestämmelser i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Av de bestämmelserna följer bl.a. att nämnden utövar sin tillsyn genom inspektioner och andra undersökningar. Vidare framgår att nämnden av de myndigheter som omfattas av tillsynen – såvitt här är av intresse Säkerhetspolisen, Rikskriminalpolisen och polismyndigheterna samt Försvarets radioanstalt – ska få det biträde och de uppgifter som nämnden begär. Även myndigheter som inte omfattas av tillsynen, t.ex. den domstol som beviljar tillstånd till signalspaning, är

skyldiga att lämna de uppgifter som nämnden begär. Slutligen framgår att nämndens beslut inte får överklagas.

Av *fjärde stycket* följer att Säkerhets- och integritetsskyddsnämnden i enskilda fall får besluta att signalspaningen ska upphöra. Det kan ske om det vid nämndens kontroll framkommer att inhämtningen inte är förenlig med lag eller författning eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten. Bestämmelsen lär få sin största betydelse i sådana fall då tillstånd till signalspaning i tråd beviljats på goda grunder, men där situationen förändrats därefter genom att nya omständigheter tillkommit eller tidigare föreliggande omständigheter ändrats eller fallit bort.

Nämnden har också enligt fjärde stycket möjlighet att besluta att upptagning eller uppteckning av inhämtade uppgifter ska förstöras. Ett sådant beslut ska grundas på motsvarande förutsättningar som när det gäller beslut om att signalspaning ska upphöra.

12 §

> Vad som föreskrivs i 11 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska tillämpas även för signalspaning enligt denna lag. Vad som där sägs om kontrollmyndigheten ska dock i stället avse Säkerhets- och integritetsskyddsnämnden.

Av 11 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet följer att det inom signalspaningsmyndigheten ska finnas ett särskilt råd med uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten. Av hänvisningen till den bestämmelsen följer att rådets verksamhet ska omfatta även den signalspaning vid signalspaningsmyndigheten som bedrivs enligt denna lag.

Rådet ska enligt den angivna bestämmelsen i lagen om signalspaning i försvarsunderrättelseverksamhet rapportera sina iakttagelser till signalspaningsmyndighetens ledning och, om rådet finner att det finns skäl för det, till den kontrollmyndighet som utövar tillsyn enligt den lagen. Rådets skyldigheter att rapportera sina iakttagelser gäller även enligt denna lag, med den skillnaden att i de fall rådet anser att det finns skäl att underrätta kontrollmyndigheten ska underrättelsen lämnas till Säkerhets- och integritetsskyddsnämnden.

Frågan har behandlats i avsnitt 7.11.2.

Hänvisningen till lagen om signalspaning i försvarsunderrättelseverksamhet avser lagen i dess föreslagna lydelse i prop. 2008/09:201 (se bilaga 2).

13 §

> Upptagningar, uppteckningar eller rapporter som gjorts vid signalspaning ska granskas av polisen snarast möjligt. De ska, i de delar de är av betydelse från brottsutredningssynpunkt, bevaras till dess förundersökningen lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar upptagningarna, uppteckningarna eller rapporterna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. De ska därefter förstöras.
>
> Beträffande upptagningar, uppteckningar eller rapporter som gjorts vid signalspaning gäller i övrigt vad som föreskrivs i 7 § 2–4 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Vad som i 7 § 4 den lagen sägs om syften med behandling av uppgifter ska dock i stället avse de syften som följer av 1, 5 och 6 §§ denna lag.
>
> Trots vad som sägs i första stycket får polisen behandla uppgifter från upptagningar, uppteckningar och rapporter i enlighet med vad som är särskilt föreskrivet i lag.

Vad som av signalspaningsmyndigheten inhämtas vid signalspaning kan från signalspaningsmyndigheten delges polisen på olika sätt. Möjligheten för signalspaningsmyndigheten att över huvud taget delge polisen sådant material är begränsad till vad som medgetts av domstolen i samband med tillståndsgivningen (se ovan kommentaren till 8 § första stycket).

Delgivningen kan ske genom att s.k. råmaterial överlämnas eller genom underrättelserapporter där materialet varit föremål för signalspaningsmyndighetens bearbetning och analys. Vilken form som väljs är naturligtvis beroende av de behov som polisen har och de alternativ som i varje fall är möjliga att åstadkomma. Valet av redovisningsform kan också ha sin grund i behovet hos signalspaningsmyndigheten att i olika avseenden hemlighålla sina metoder och sin förmåga. Signalspaningsmyndigheten får som nämnts ovan självfallet inte redovisa annan information än vad som medges av domstolens tillstånd.

I paragrafen behandlas vad som ska ske med upptagningar, uppteckningar eller rapporter som härrör från signalspaning och som överlämnats av signalspaningsmyndigheten till polisen. Bestämmelserna i *första och tredje styckena* motsvarar vad som gäller enligt reglerna om polisens användning av hemlig teleavlyssning (jfr 27 kap. 24 § rättegångsbalken).

Genom den hänvisning till lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet som följer av andra stycket kommer emellertid förstöringsskyldigheten enligt denna lag att bli mer omfattande än vad som följer av bestämmelserna om hemliga tvångsmedel. Dessa särskilda grunder för förstöring har behandlats i avsnitt 7.9.2.

Hänvisningen till lagen om signalspaning i försvarsunderrättelseverksamhet avser lagen i dess föreslagna lydelse i prop. 2008/09:201 (se bilaga 2).

14 §

> Om underrättelser som inhämtats genom signalspaning enligt denna lag kan antas vara av särskild betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, får uppgifterna överlämnas till regeringen, Regeringskansliet eller Försvarsmakten. Om uppgifterna inhämtats inom ramen för en förundersökning får ett sådant överlämnande ske endast om förundersökningsledaren medgivit det.

Bestämmelserna i paragrafen reglerar den situationen att det vid signalspaning som utförs för polisen räkning framkommer information som kan antas vara av särskild betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

Uppgifter som bedöms ha sådan betydelse får, utan hinder av sekretess, överlämnas till de myndigheter som föreslås få inrikta signalspaningen inom försvarsunderrättelseverksamheten. Eventuell sekretess hindrar självfallet inte att uppgifter överlämnas till regeringen. Regeringen nämns i bestämmelsen därmed enbart i ett tydliggörande syfte.

Av bestämmelser i förordning bör framgå att frågan om att överlämna sådan information avgörs av signalspaningsmyndigheten efter samråd med Rikspolisstyrelsen.

För det fall informationen har inhämtats inom ramen för en förundersökning får den inte överlämnas utan tillstånd av förundersökningsledaren.

Det kan nämnas att i det omvända fallet, dvs. att det vid signalspaning inom försvarsunderrättelseverksamheten inhämtas information som visar sig ha betydelse för polisen, finns möjlighet att med stöd av 2 § första stycket lagen (2000:130) om försvarsunderrättelseverksamhet överlämna sådan information till polisen.

Frågan har behandlats i avsnitt 7.9.4.

15 §

Vad som föreskrivs i 9 § andra stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska gälla även för verksamhet som signalspaningsmyndigheten bedriver enligt 3 § tredje stycket denna lag.

Av 3 § tredje stycket denna lag följer att signalspaningsmyndigheten får bedriva signalspaning med syftet att tillgodose myndighetens egna behov av teknik- och kompetensutveckling.

Av 9 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet följer att signalspaningsmyndigheten för sådan verksamhet får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer. Genom hänvisningen till den paragrafen ges signalspaningsmyndigheten en möjlighet till sådant samarbete även beträffande den verksamhet som myndigheten bedriver enligt denna lag.

Hänvisningen till lagen om signalspaning i försvarsunderrättelseverksamhet avser lagen i dess föreslagna lydelse i prop. 2008/09:201 (se bilaga 2).

16 §

I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om operatörers skyldighet att överföra signaler för att möjliggöra inhämtning enligt denna lag.

Endast den myndighet som avses i 12 § andra stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska ha rådighet över signalbärare innehållande sådana signaler som överförs i enlighet med de bestämmelser som avses i första stycket. Myndigheten ska ge signalspaningsmyndigheten tillgång till signalbärare endast i den utsträckning som följer av tillstånd enligt 8–10 §§ denna lag.

Paragrafen innehåller i *första stycket* en hänvisning till de bestämmelser i lagen (2003:389) om elektronisk kommunikation som reglerar teleoperatörernas skyldighet att överföra signaler för att möjliggöra signalspaning i tråd enligt denna lag. En motsvarande bestämmelse finns intagen i 12 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

I andra stycket regleras rådigheten över de signaler i tråd som av operatörer överförs till samverkanspunkter. Det är samma myndighet som har rådigheten över signalbärarna enligt lagen om signalspaning i

försvarsunderrättelseverksamhet som har rådigheten enligt denna lag. Myndigheten ska ge signalspaningsmyndigheten tillgång till signalbärare i enlighet med domstolens tillstånd eller enligt ett sådant beslut om signalspaning som kan fattas i brådskande fall. När ett tillstånd föreligger ska myndigheten inte göra någon prövning av förutsättningarna utan endast verkställa vad som framgår av tillståndet eller beslutet.

Hänvisningen till lagen om signalspaning i försvarsunderrättelseverksamhet avser lagen i dess föreslagna lydelse i prop. 2008/09:201 (se bilaga 2).

9.2 Förslaget till ändring i lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

1 §

Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt i myndighetens verksamhet enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen (1998:204) gäller inte vid sådan behandling av personuppgifter som anges i första stycket.

Genom ett tillägg i paragrafen har lagens tillämpningsområde breddats till att även avse Försvarets radioanstalts verksamhet enligt lagen om signalspaning för polisens behov avseende utrikes förhållanden.

2 §

Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt i myndighetens verksamhet enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden.

Genom ett tillägg i paragrafen har syftet med lagen breddats till att också omfatta myndighetens verksamhet enligt lagen om polisens signalspanig avseende utrikes förhållanden.

7 §

I Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt i myndighetens verksamhet enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden får, under de förutsättningar som anges i denna lag, personuppgifter behandlas i uppgiftssamlingar.

Regeringen meddelar närmare föreskrifter eller beslut i enskilda fall om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling.

Genom ett tillägg i paragrafens första stycke klargörs att Försvarets radioanstalt även avseende den verksamhet som bedrivs enligt lagen om signalspaning för polisens behov avseende utrikes förhållanden får behandla personuppgifter i uppgiftssamlingar.

8 a §

Personuppgifter får behandlas i Försvarets radioanstalts verksamhet enligt lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden om det är nödvändigt för den verksamheten.

Paragrafen är ny. Lagen innehåller redan i 8 och 9 §§ bestämmelser om rätten för Försvarets radioanstalt att behandla personuppgifter i sin försvarsunderrättelse- och utvecklingsverksamhet. Den nya paragrafen ger Försvarets radioanstalt en motsvarande rätt att behandla personuppgifter i verksamhet enligt lagen om signalspaning för polisens behov avseende utrikes förhållanden. Rätten att behandla personuppgifter är begränsad till de fall då det är nödvändigt för verksamhet enligt den lagen.

9.3 Förslaget till ändring i lagen om elektronisk kommunikation

6 kap. 19 a §

För att inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden skall kunna ske, är operatörer som äger tråd i vilka signaler förs över Sveriges gräns skyldiga att överföra dessa till samverkanspunkter. Varje sådan operatör skall anmäla en eller flera samverkanspunkter till den myndighet som regeringen bestämmer. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om samverkanspunkter.

Samtliga operatörer som för signaler i tråd över Sveriges gräns skall till den myndighet som regeringen bestämmer lämna sådan information de innehar som gör det enklare att ta hand om signalerna.

Samtliga operatörer skall utföra uppgifterna enligt första och andra stycket så att verksamheten inte röjs.

Paragrafen har ändrats på det sättet att operatörernas skyldigheter också omfattar den signalspaning som bedrivs enligt lagen om signalspaning för polisens behov avseende utrikes förhållanden. Vad gäller kommentarer kring innebörden av operatörernas skyldigheter hänvisas till vad regeringen anfört i prop. 2006/07:63 s. 142 f.

6 kap. 21 §

Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till

1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,
2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken eller tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål, och
3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och lagen (0000:000) om signalspaning för polisens behov avseende utrikes förhållanden.

Paragrafen har ändrats på det sättet att i punkten 3 har tillagts lagen om signalspaning för polisens behov avseende utrikes förhållanden. Ändringen innebär att den tystnadsplikt som gäller för operatörerna avseende angelägenhet som avser inhämtning genom signal-

spaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet också gäller för sådan angelägenhet vid signalspaning enligt lagen om signalspaning för polisens behov avseende utrikes förhållanden.

Kommittédirektiv

Underrättelseinhämtning för vissa polisiära behov

Dir. 2008:120

Beslut vid regeringssammanträde den 9 oktober 2008

Sammanfattning av uppdraget

Mot bakgrund av att Försvarets radioanstalt endast kommer att bedriva signalspaning i försvarsunderrättelseverksamhet enligt den inriktning som regeringen, Regeringskansliet och Försvarsmakten bestämmer, uppdras åt en särskild utredare att

- kartlägga Säkerhetspolisens och Rikskriminalpolisens behov av underrättelser om utländska förhållanden,
- utreda hur detta behov ska kunna tillgodoses på ett rättssäkert och effektivt sätt, och
- lämna fullständiga författningsförslag i frågan.

Utredaren ska redovisa uppdraget senast den 30 juni 2009.

Bakgrund

En grundläggande statlig uppgift är att skydda landet mot bl.a. terrorism och andra hot mot rikets säkerhet. Ett viktigt verktyg i det arbetet är underrättelseinhämtning.

Försvarets radioanstalt har i hög grad bidragit till underrättelseinhämtningen om utländska förhållanden när det gäller bl.a. internationell terrorism, annan grov gränsöverskridande brottslighet och främmande underrättelseverksamhet mot svenska intressen. Underrättelser som inhämtats inom ramen för försvarsunderrättelseverksamheten har rapporterats till Säkerhetspolisen och Rikskriminalpolisen och utgjort ett viktigt underlag för myndigheternas verksamhet.

Behovet av en utredning

Den 1 januari 2009 träder nya regler i kraft för signalspaning i försvarsunderrättelseverksamhet. Från och med den 1 oktober 2009 är det möjligt att inom ramen för sådan verksamhet signalspana mot trådburen kommunikation.

Under hösten 2008 har en politisk överenskommelse träffats som innebär förändringar i förhållande till de nya bestämmelserna. Förändringarna medför att Försvarets radioanstalt endast kommer att få bedriva signalspaning enligt den inriktning som regeringen, Regeringskansliet och Försvarsmakten bestämmer. Denna förändring väcker frågor om hur Säkerhetspolisens och Rikskriminalpolisens behov av underrättelser om utländska förhållanden när det gäller bl.a. internationell terrorism, annan grov gränsöverskridande brottslighet och främmande underrättelseverksamhet mot svenska intressen ska kunna tillgodoses.

Uppdraget

En särskild utredare tillkallas med uppdrag att kartlägga Säkerhetspolisens och Rikskriminalpolisens behov av underrättelseinhämtning avseende utländska förhållanden genom signalspaning. Mot bakgrund av kartläggningen ska utredaren, med beaktande av skyddet för den enskildes personliga integritet och med beaktande av Sveriges internationella åtaganden och övriga internationella samarbete, överväga och föreslå hur detta behov ska kunna tillgodoses på ett rättssäkert och effektivt sätt. Förslagen ska utformas så att förhållandet mellan signalspaning i försvarsunderrättelseverksamhet och motsvarande underrättelseinhämtning i polisiär verksamhet tydliggörs. Vid genomförandet av uppdraget ska utredaren beakta utformningen av motsvarande system i jämförbara länder.

Utredaren ska överväga alternativa lösningar för att verkställa underrättelseinhämtningen och uppskatta kostnaderna för de olika alternativen.

Utredaren ska utarbeta fullständiga författningsförslag.

Utredaren är fri att ta upp och lämna förslag i näraliggande frågor som aktualiseras under utredningsarbetet.

Uppdragets genomförande

Utredaren ska samråda med berörda myndigheter.

Till stöd för utredarens arbete ska en referensgrupp med representanter för riksdagspartierna inrättas.

Utredaren ska hålla sig informerad om arbetet inom Regeringskansliet med att ta fram kompletterande lagstiftning till lagen (2008:717) om signalspaning.

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Uppdraget ska redovisas senast den 30 juni 2009.

(Justitiedepartementet)

Förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

Härigenom föreskrivs i fråga om lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

dels att 1 och 3–12 §§ ska ha följande lydelse,

dels att det i lagen ska införas åtta nya paragrafer, 2 a , 4 a , 5 a, 5 b, 10 a, 11 a, 11 b och 12 a §§, samt närmast före 1, 3, 4, 4 a, 7, 8, 9, 10, 11 a och 12 §§ nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	Signalspaningens omfattning
	1 §
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.	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 *en myndighet som anges i 4 §* närmare har bestämt inriktningen av signalspaningen. *Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att kartlägga* *1. yttre militära hot mot landet,* *2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av*

sådana insatser,

3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,

4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,

5. allvarliga yttre hot mot samhällets infrastrukturer,

6. konflikter utomlands med konsekvenser för internationell säkerhet,

7. främmande underrättelseverksamhet mot svenska intressen, eller

8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

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.

2 a §

Inhämtning får inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats.

	Första stycket tillämpas inte i fråga om signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg eller militära fordon.
	Sökbegrepp
3 §	
Inhämtning av signaler i tråd *skall* ske automatiserat. Sådan inhämtning får endast avse signaler som identifierats genom sökbegrepp. Även vid annan automatiserad inhämtning *skall* sökbegrepp användas för identifiering av signaler.	Inhämtning av signaler i tråd *ska* ske automatiserat. Sådan inhämtning får avse endast signaler som identifierats genom sökbegrepp. Även vid annan automatiserad inhämtning *ska* sökbegrepp användas för identifiering av signaler.
Sökbegreppen *skall* utformas och användas så att *de* medför ett så begränsat *intrång* som möjligt *i den personliga integriteten*. *Sökbegreppen får inte vara* direkt hänförliga till en viss fysisk person *om det inte* är av synnerlig vikt för verksamheten.	Sökbegreppen *ska* utformas och användas *med respekt för enskildas personliga integritet och* så att *signalspaningen* medför ett så begränsat *integritetsintrång* som möjligt. *För sökbegrepp som är* direkt hänförliga till en viss fysisk person *gäller därutöver att de får användas endast om det* är av synnerlig vikt för verksamheten.
	Inriktning
4 §	
I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. *En inriktning av signalspaningen får inte avse endast en viss fysisk person.*	I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. *Inriktning av signalspaning får anges endast av regeringen, Regeringskansliet och Försvarsmakten.*
Regeringen bestämmer inriktningen av den verksamhet som bedrivs enligt 1 § *andra* stycket.	Regeringen bestämmer inriktningen av den verksamhet som bedrivs enligt 1 § *tredje* stycket.

Regeringens beslut om inriktning av signalspaningsverksamheten skall föregås av samråd med den myndighet som avses i 6 §.

En inriktning av signalspaningen får inte avse endast en viss fysisk person.

Tillstånd

4 a §

Signalspaningsmyndigheten ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för signalspaning enligt 1 §. En sådan ansökan ska innehålla uppgifter om

1. det inhämtningsuppdrag som ansökan avser, med en närmare redogörelse för det behov som föranleder ansökan och uppgift om vilken inriktning uppdraget hänför sig till,

2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget,

3. de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas vid inhämtningen,

4. vilken tid tillståndet ska gälla, och

5. de omständigheter i övrigt som myndigheten vill åberopa till stöd för sin ansökan.

5 §

För en myndighets närmare inriktning av signalspaning enligt 1 § första stycket krävs tillstånd, om inte inriktningen har angetts av regeringen eller Regeringskansliet. Ett tillstånd får ges för högst sex månader från dagen för beslutet och kan efter förnyad prövning förlängas

Tillstånd för signalspaning enligt visst inhämtningsuppdrag får lämnas endast om

1. uppdraget är förenligt med lagen (2000:130) om försvarsunderrättelseverksamhet och denna lag,

2. syftet med inhämtningen inte

med högst sex månader i taget.

Tillstånd får endast ges för inriktning som är förenlig med lagen (2000:130) om försvarsunderrättelseverksamhet. Tillstånd får endast lämnas om syftet med inriktningen väger klart tyngre än det integritetsintrång som inhämtning i enlighet med inriktningen kan innebära och detta syfte inte kan tillgodoses på ett mindre ingripande sätt. Tillstånd får inte lämnas om inriktningen endast avser en viss fysisk person.

I brådskande fall får inriktning anges utan att tillstånd har lämnats. Inriktningen skall då omedelbart anmälas till den myndighet som skall lämna tillstånd. Finner tillståndsmyndigheten att det saknas förutsättningar för tillstånd, skall signalspaningsmyndigheten underrättas. Verksamheten med anledning av inriktningen skall då omedelbart avbrytas.

kan tillgodoses på ett mindre ingripande sätt,

3. uppdraget beräknas ge information vars värde är klart större än det integritetsintrång som inhämtning i enlighet med ansökan kan innebära,

4. de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas är förenliga med 3 §, och

5. ansökan inte avser endast en viss fysisk person.

5 a §

I ett tillstånd ska anges

1. det inhämtningsuppdrag för vilket inhämtning får ske,

2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten ska få tillgång till för att fullgöra uppdraget,

3. vilka sökbegrepp eller kategorier av sökbegrepp som får användas vid inhämtningen,

4. den tid som tillståndet avser, och

5. de villkor i övrigt som behövs

för att begränsa intrånget i enskildas personliga integritet.

Ett tillstånd får ges för högst sex månader från dagen för beslutet och kan efter förnyad prövning förlängas med högst sex månader i taget.

Om det för fullgörande av inhämtningsuppdrag för vilket tillstånd givits uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp, ska särskilt tillstånd sökas. Vid ansökan och prövning gäller 4 och 5 §§ i tillämpliga delar. Ett sådant tillstånd ska ha samma varaktighet som tillståndet för det inhämtningsuppdrag inom vilket tillgång till signalerna behövs eller sökbegreppen är avsedda att användas.

5 b §

Om det kan befaras att inhämtande av Försvarsunderrättelsedomstolens tillstånd skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för något av de i 1 § angivna syftena, får tillstånd till signalspaningen ges av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver. Ett sådant tillstånd ska utformas i enlighet med 5 a §.

Har tillstånd lämnats enligt första stycket ska åtgärden genast anmälas skriftligen till Försvarsunderrättelsedomstolen. I anmälan ska skälen för åtgärden anges. Försvarsunderrättelsedomstolen ska

skyndsamt pröva ärendet och, om den finner att det inte finns skäl för åtgärden, upphäva eller ändra beslutet. Om ett beslut enligt första stycket har upphört att gälla innan domstolen har prövat ärendet, ska signalspaningsmyndigheten anmäla åtgärden till kontrollmyndigheten.	
Om Försvarsunderrättelsedomstolen upphäver eller ändrar ett beslut enligt första stycket ska upptagning eller uppteckning av uppgifter som redan inhämtats omgående förstöras i den utsträckning upptagningen eller uppteckningen kan hänföras till ändringen.	
6 §	
Tillstånd enligt 5 § lämnas av den myndighet som regeringen bestämmer. Myndigheten skall vara fristående från signalspaningsmyndigheten. Prövning av tillstånd skall ske i en enhet inom myndigheten vars ledamöter utses av regeringen för en bestämd tid, minst fyra år. Ordföranden och vice ordföranden skall vara eller ha varit ordinarie domare. Övriga ledamöter skall utses bland personer som föreslagits av partigrupperna i riksdagen.	*Bestämmelser om Försvarsunderrättelsedomstolen finns i lagen (2009:000) om Försvarsunderrättelsedomstol.*
	Förstöringsskyldighet
7 §	
Upptagning eller uppteckning av uppgifter som inhämtats enligt denna lag *skall* omgående förstöras om innehållet	Upptagning eller uppteckning av uppgifter som inhämtats enligt denna lag *ska* omgående förstöras om innehållet
1. berör en viss fysisk person och har bedömts sakna betydelse	1. berör en viss fysisk person och har bedömts sakna betydelse

för verksamhet som avses i 1 §,

2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 4 § tryckfrihetsförordningen eller 2 kap. 4 § yttrandefrihetsgrundlagen, *eller*

3. omfattar uppgifter i meddelanden som avses i 27 kap. 22 § rättegångsbalken.

för verksamhet som avses i 1 §,

2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 4 § tryckfrihetsförordningen eller 2 kap. 4 § yttrandefrihetsgrundlagen,

3. omfattar uppgifter i meddelanden som avses i 27 kap. 22 § rättegångsbalken, *eller*

4. avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för syften som anges i 1 § andra stycket.

Rapportering

8 §

Underrättelser med uppgifter som inhämtats enligt denna lag *skall* rapporteras till berörda myndigheter i enlighet med vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet.

Om uppgifterna berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § den lagen.

Underrättelser med uppgifter som inhämtats enligt denna lag *ska* rapporteras till berörda myndigheter i enlighet med vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet. Om uppgifterna berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § den lagen.

Internationellt samarbete

9 §

Signalspaningsmyndigheten får för den verksamhet som anges i 1 § *andra* stycket, enligt regeringens närmare bestämmande, etablera och upprätthålla sam-

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om internationellt samarbete på försvarsunderrättelseområdet.

arbete i signalspaningsfrågor med andra länder och internationella organisationer.

Signalspaningsmyndigheten får för den verksamhet som anges i 1 § *tredje* stycket, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.

Kontroll

10 §

Den myndighet som regeringen bestämmer *skall* kontrollera att denna lag följs. Kontrollen *skall* särskilt avse granskning av sökbegrepp som avses i 3 §, förstöring av uppgifter som avses i 7 § samt rapportering enligt 8 §.

Myndigheten får besluta att viss inhämtning *skall* upphöra eller att upptagning eller uppteckning av inhämtade uppgifter *skall* förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med denna lag eller *annars utgör ett* intrång i enskildas rättig heter som inte står i rimlig proportion till syftet med verksamheten.

Beslut enligt andra stycket skall fattas av en enhet inom myndigheten vars ledamöter utses av regeringen för en bestämd tid, minst fyra år. Ordföranden och vice ordföranden *skall* vara eller ha varit ordinarie domare. Övriga ledamöter *skall* utses bland personer som föreslagits av partigrupperna i riksdagen. *Om uppgifterna enligt denna paragraf och 6 § fullgörs av samma myndighet, får de ledamöter*

Den myndighet som regeringen bestämmer *(kontrollmyndigheten) ska* kontrollera att denna lag följs. Kontrollen *ska* särskilt avse granskning av sökbegrepp som avses i 3 §, förstöring av uppgifter som avses i 7 § samt rapportering enligt 8 §.

Myndigheten får besluta att viss inhämtning *ska* upphöra eller att upptagning eller uppteckning av inhämtade uppgifter *ska* förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med *tillstånd meddelat enligt* denna lag.

Myndigheten ska ledas av en nämnd vars ledamöter utses av regeringen för en bestämd tid, minst fyra år. Ordföranden och vice ordföranden *ska* vara eller ha varit ordinarie domare. Övriga ledamöter *ska* utses bland personer som föreslagits av partigrupperna i riksdagen.

som prövar frågor om tillstånd inte delta vid beslut enligt andra stycket.

10 a §
Kontrollmyndigheten är skyldig att på begäran av en enskild kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning enligt denna lag och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Kontrollmyndigheten ska underrätta den enskilde om att kontrollen har utförts.

11 §

Inom signalspaningsmyndigheten *skall* det finnas ett råd med uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten. Rådets ledamöter utses av regeringen för viss tid. Rådet *skall* rapportera sina iakttagelser till signalspaningsmyndighetens ledning och, om rådet finner att det finns skäl för det, till *den myndighet som avses i 10 §*.

Inom signalspaningsmyndigheten *ska* det finnas ett råd med uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten. Rådets ledamöter utses av regeringen för viss tid. Rådet *ska* rapportera sina iakttagelser till signalspaningsmyndighetens ledning och, om rådet finner att det finns skäl för det, till *kontrollmyndigheten*.

Underrättelseskyldighet
11 a §
Om det vid signalspaning enligt denna lag har använts sökbegrepp som är direkt hänförliga till en viss fysisk person, ska personen underrättas om detta, om inte annat följer av 11 b §. Underrättelsen ska innehålla uppgift om när inhämtningen

skett och syftet med inhämtningen.

En underrättelse ska lämnas så snart det kan ske utan men för försvarsunderrättelseverksamheten, dock senast en månad efter att det inhämtningsuppdrag som föranlett inhämtningen avslutades.

11 b §

Underrättelse enligt 11 a § får skjutas upp, om sekretess hindrar att underrättelsen lämnas. Har det på grund av sekretess inte kunnat lämnas någon underrättelse inom ett år från det att inhämtningsuppdraget avslutades, behöver någon underrättelse inte lämnas.

En underrättelse ska inte lämnas om inhämtningen uteslutande avser främmande makts förhållanden eller förhållanden mellan främmande makter.

Övriga bestämmelser

12 §

I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om operatörers skyldighet att överföra signaler för att möjliggöra inhämtning enligt denna lag.

Endast kontrollmyndigheten ska ha rådighet över signalbärare innehållande sådana signaler som överförs i enlighet med de bestämmelser som avses i första stycket. Myndigheten ska ge signalspaningsmyndigheten tillgång till signalbärare endast i den utsträckning det följer av tillstånd enligt 5 a eller 5 b §.

12 a §

I lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter.

---

1. Denna lag träder i kraft den 1 december 2009.
2. Verksamhet som vid ikraftträdandet bedrivs med stöd av tillstånd meddelade enligt äldre bestämmelser får bedrivas till dess att tiden för tillståndet löper ut.

Statens offentliga utredningar 2009

Kronologisk förteckning

1. En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen. Ju.
2. Nya nät för förnybar el. N.
3. Ransonering och prisreglering i krig och fred. Fö.
4. Sekretess vid anställning av myndighetschefer. Fi.
5. Säkerhetskopiors rättsliga status. Ju.
6. Återkrav inom välfärdssystemen. – Förslag till lagstiftning. Fi.
7. Den svenska administrationen av jordbruksstöd. Jo.
8. Trygg med vad du äter – nya myndigheter för säkra livsmedel och hållbar produktion. Jo.
9. Säkerhetskontroller vid fullmäktige- och nämndsammanträden. Fi.
10. Miljöprocessen. M.
11. En nationell cancerstrategi för framtiden. S.
12. Skatt i retur. Fi.
13. Effektiviteten i Kriminalvårdens lokalförsörjning. Ju.
14. Grundlagsskydd för digital bio och andra yttrandefrihetsrättsliga frågor. Ju.
15. Kraftsamling! – museisamverkan ger resultat. + Bilagor. Ku.
16. Betänkande av Kulturutredningen. Grundanalys Förnyelseprogram Kulturpolitikens arkitektur. Ku.
17. Kommunal kompetenskatalog. En problemorientering. Ju.
18. Två rapporter till Grundlagsutredningen. Ju.
19. Aktiv väntan – asylsökande i Sverige. Ju.
20. Mer järnväg för pengarna. N.
21. Redovisning av kommunal medfinansiering. Fi.
22. En ny alkohollag. S.
23. Olovlig tobaksförsäljning. S.
24. De statliga beställarfunktionerna och anläggningsmarknaden. N.
25. Samordnad kommunstatistik för styrning och uppföljning. Fi.
26. Det växande vattenbrukslandet. Jo.
27. Ta klass. U.
28. Stärkt stöd för studier – tryggt, enkelt och flexibelt. + Bilagor. U.
29. Fritid på egna villkor. IJ.
30. Skog utan gräns? Jo.
31. Effektiva transporter och samhällsbyggande – en ny struktur för sjö, luft, väg och järnväg. N.
32. Socialtjänsten. Integritet – Effektivitet. S.
33. Skatterabatt på aktieförvärv och vinstutdelningar. Fi.
34. Förenklingar i aktiebolagslagen m.m. Ju.
35. Moderna hyreslagar. Ju.
36. Främja, Skydda, Övervaka – FN:s konvention om rättigheter för personer med funktionsnedsättning. IJ.
37. Enklare beslutsfattande i ekonomiska föreningar. Ju.
38. Ingen får vara Svarte Petter. Tydligare ansvarsfördelning inom socialtjänsten. S.
39. En ny kollektivtrafiklag. + Bilagor. N.
40. En ny modell för arbetsmiljötillsyn. A.
41. Bättre och snabbare insättningsgaranti. Fi.
42. Vattenverksamhet. M.
43. Klinisk forskning – ett lyft för sjukvården. U.
44. Integritetsskydd i arbetslivet. A.
45. Områden av riksintresse och Miljökonsekvensbeskrivningar. M.
46. Försenad årsredovisning och bokföringsbrott, m.m. Ju.
47. God arbetsmiljö - en framgångsfaktor? A
48. Koncessioner för el- och gasnät. N.

49. Bättre samverkan. Några frågor kring samspelet mellan sjukvård och social-försäkring. S.
50. Nytt pensionssystem för den statsunder stödda scenkonsten. Fi.
51. Avskaffande av filmcensuren för vuxna – men förstärkt skydd för barn och unga mot skadlig mediepåverkan. Ku.
52. Staten och imamerna. Religion, integration, autonomi. U.
53. Fiskevård i enskilt vatten. En översyn av lagen om fiskevårdsområden. Jo.
54. Uthållig älgförvaltning i samverkan. Jo.
55. Ett effektivare smittskydd. S.
56. Den nya migrationsprocessen. Ju.
57. Myndighet för hållbart samhällsbyggande – en granskning av Boverket. M.
58. Skatteförfarandet. Fi.
59. Skatteincitament för gåvor till forskning och ideell verksamhet. Fi.
60. Återvändandedirektivet och svensk rätt. Ju.
61. Modernare adoptionsregler. Ju.
62. Skatt på fluorerade växthusgaser. Fi.
63. Totalförsvarsplikt och frivillighet. Fö.
64. Flickor och pojkar i skolan - hur jämställt är det? U.
65. Moderniserade skatteregler för ideell sektor. Fi.
66. Signalspaning för polisiära behov. Ju.

Statens offentliga utredningar 2009

Systematisk förteckning

Det växande vattenbrukslandet. [26]
Skog utan gräns? [30]
Fiskevård i enskilt vatten. En översyn av lagen om fiskevårdsområden. [53]
Uthållig älgförvaltning i samverkan. [54]

Miljödepartementet

Miljöprocessen. [10]
Vattenverksamhet. [42]
Områden av riksintresse och Miljökonsekvensbeskrivningar. [45]
Myndighet för hållbart samhällsbyggande – en granskning av Boverket. [57]

Näringsdepartementet

Nya nät för förnybar el. [2]
Mer järnväg för pengarna. [20]
De statliga beställarfunktionerna och anläggningsmarknaden. [24]
Effektiva transporter och samhällsbyggande – en ny struktur för sjö, luft, väg och järnväg. [31]
En ny kollektivtrafiklag. + Bilagor. [39]
Koncessioner för el- och gasnät. [48]

Integrations- och jämställdhetsdepartementet

Fritid på egna villkor. [29]
Främja, Skydda, Övervaka – FN:s konvention om rättigheter för personer med funktionsnedsättning. [36]

Kulturdepartementet

Kraftsamling! – museisamverkan ger resultat. + Bilagor. [15]
Betänkande av Kulturutredningen.
Grundanalys
Förnyelseprogram
Kulturpolitikens arkitektur. [16]
Avskaffande av filmcensuren för vuxna – men förstärkt skydd för barn och unga mot skadlig mediepåverkan. [51]

Arbetsmarknadsdepartementet

En ny modell för arbetsmiljötillsyn. [40]
Integritetsskydd i arbetslivet. [44]
God arbetsmiljö - en framgångsfaktor? [47]