Regeringens proposition till riksdagen med förslag till lagstiftning om civil underrättelseinhämtning

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att det stiftas en ny lag om civil underrättelseinhämtning avseende datatrafik och att polislagen ändras så att ett nytt kapitel fogas till lagen. I det nya kapitlet föreslås bestämmelser om metoder för underrättelseinhämtning och användning av dem vid civil underrättelseinhämtning. Dessutom föreslås det att polisförvaltningslagen, lagen om behandling av personuppgifter i polisens verksamhet, strafflagen, förundersökningslagen, tvångsmedelslagen och lagen om offentlighet vid rättegång i allmänna domstolar ändras. Propositionen hänför sig till de regeringspropositioner som överlämnas samtidigt och i vilka det föreslås att det stiftas en ny lag om militär underrättelseverksamhet och en ny lag om övervakning av underrättelseverksamheten.

Det viktigaste målet med den lagstiftning som föreslås i denna proposition är att förbättra den nationella säkerheten och att skapa en rättsgrund för underrättelseinhämtning. Målsättningen är att förbättra det finländska samhällets möjligheter att skydda sig mot de allra allvarligaste hoten som riktas mot den nationella säkerheten. Dessa utgörs av sådana objekt för civil underrättelseinhämtning som definieras uttömmande i lagen. Vid beredningen av lagförslagen har strävan varit att begränsa ingripandet i skyddet för de grundläggande fri- och rättigheterna så att det sker i så liten utsträckning som möjligt med beaktande av kraven på att underrättelseverksamheten ska vara effektiv och ge resultat.

De föreslagna bestämmelserna om metoder för underrättelseinhämtning baserar sig metod- och definitionsmässigt delvis på de hemliga metoder för inhämtande av information som det föreskrivs om i polislagen. Som metoder för underrättelseinhämtning räknas dessutom platsspecifik underrättelseinhämtning, kopiering, kvarhållande av försändelser för kopiering och rätt att få information av privata sammanslutningar samt underrättelseinhämtning som avser datatrafik. Syftet med de olika metoderna för underrättelseinhämtning är att till stöd för den högsta statsledningens beslutsfattande och till skydd för den nationella säkerheten producera nödvändig information om verksamhet som allvarligt hotar den nationella säkerheten. Ett särskilt mål för underrättelseinhämtning som avser datatrafik är att förbättra Finlands förmåga att skydda sig mot de allvarligaste cyberhoten.

De föreslagna bestämmelserna om beslutsfattande i fråga om metoderna för underrättelseinhämtning baserar sig också delvis på det kapitel i polislagen som gäller hemliga metoder för inhämtande av information. Beslut om underrättelseinhämtning som avser datatrafik ska fattas av domstol. Domstolen ska också besluta om platsspecifik underrättelseinhämtning när den riktas mot en hemfridsskyddad plats eller mot en plats som man inte har allmänt tillträde till eller om det allmänna tillträdet till den har begränsats eller förhindrats. Chefen för skyddspolisen ska besluta om underrättelseinhämtning som avser utländska förhållanden, om användning av metoder för underrättelseinhämtning som avser utländska förhållanden och om deltagande i internationellt samarbete.

Information som fåtts genom metoder för underrättelseinhämtning ska under vissa förutsättningar kunna lämnas ut till förundersökningsmyndigheter eller andra behöriga myndigheter. På grund av den ändamålsbundenhet som gäller informationen föreslås det strikta villkor för utlämnande av information.

I polislagen föreslås bestämmelser om samarbete med militärunderrättelsemyndigheten och andra myndigheter samt om samordning av hemligt inhämtande av information för att säkerställa arbetssäkerheten för tjänstemännen vid skyddspolisen, militärunderrättelsemyndigheten, centralkriminalpolisen och andra myndigheter.

I polislagen och i lagen om civil underrättelseinhämtning avseende datatrafik föreslås bestämmelser om kopieringsförbud, förbud mot avlyssning och observation samt förbud mot underrättelseinhämtning. Vissa yrkesgruppers kommunikation ska omfattas av ett utvidgat skydd mot civil underrättelseinhämtning. Om vissa villkor uppfylls, ska de som är föremål för inhämtningen underrättas om användningen av metoder för underrättelseinhämtning.

För att garantera en rättvis rättegång föreslås det att skyddspolisens befogenheter att göra förundersökningar och använda tvångsmedel slopas när skyddspolisens befogenheter i fråga om underrättelseinhämtning utökas. Detta hindrar inte skyddspolisen från att i egenskap av expertmyndighet eventuellt delta i en förundersökning som görs av en förundersökningsmyndighet.

De ökade befogenheterna för underrättelseinhämtning och de sannolikt ökade resurserna innebär att betydelsen av den laglighetsövervakning som skyddspolisen omfattas av får en starkare framtoning. I denna proposition föreslås det att övervakningen av skyddspolisens verksamhet effektiviseras. Skyddspolisen ska informera underrättelseombudsmannen om tillstånd eller beslut som gäller metoder för underrättelseinhämtning så snart som möjligt efter det att tillståndet beviljats eller beslutet fattats. Skyddspolisen ska också så snart som möjligt informera underrättelseombudsmannen om skyddande av civil underrättelseinhämtning, yppandeförbud och beslut om fördröjning av utlämnande av information för brottsbekämpning.

I den proposition med förslag till lagstiftning om övervakning av underrättelseverksamheten som har samband med denna proposition föreslås det att det inrättas en oavhängig juridisk övervakningsmyndighet, en underrättelseombudsman, som ska övervaka underrättelseverksamheten i realtid.

Propositionen hänför sig också till en proposition med förslag till ändring av grundlagen. Befogenheter som ingriper i skyddet för förtroliga meddelanden anknyter till den föreslagna grundlagsändringen.

Alla regeringspropositioner som hänför sig till underrättelseverksamheten är beroende av varandra och bör föreläggas grundlagsutskottet samtidigt.

Lagarna avses träda i kraft så snart som möjligt.

———————

INNEHÅLL

ALLMÄN MOTIVERING

1 Inledning

Under de senaste åren har Finlands säkerhetspolitiska omgivning förändrats och digitaliserats i betydande grad. Hoten mot den inre och den yttre säkerheten flyter allt mer in i varandra. De allvarligaste hoten mot den nationella säkerheten är nästan utan undantag av internationellt ursprung eller har kopplingar till områden utanför vårt land. Av hotens internationella karaktär följer att aktörerna bakom dem har bildat nätverk på olika länders territorium. De som är delaktiga kommunicerar över statsgränserna. Den snabba kommunikationstekniska utvecklingen har effektiviserat och underlättat gränsöverskridande kontakter och nätverkande för de aktörer som utgör ett hot mot Finland samt snabbat upp internationaliseringen av hoten. Det har blivit svårare att identifiera statliga och icke-statliga aktörer bakom hoten och att förutse deras verksamhet. It-utvecklingen har gett även små stater och icke-statliga aktörer möjlighet att agera effektivt. Den teknologiska utvecklingen har gjort det möjligt att efter en allt kortare tid av förberedelser och med allt allvarligare konsekvenser genomföra gärningar som äventyrar den nationella säkerheten. Attacker som genomförs i datanät kan användas som verktyg för politisk och ekonomisk påtryckning och i en allvarlig kris som en påverkningsmetod utöver militära maktmedel.

De myndigheter som ansvarar för den nationella säkerheten har till uppgift att inom sitt ansvarsområde förutse och förebygga sådana skadliga gärningar och åtgärder som kan äventyra nationella intressen som anses vara speciellt viktiga. Allvarliga säkerhetshot kan riktas mot Finland från områden utanför Finlands gränser. Datanätens utveckling har minskat det fysiska avståndets betydelse när det gäller att förverkliga hoten. De myndigheter som ansvarar för den nationella säkerheten inhämtar underrättelser som krävs för att de ska kunna fullgöra sina lagstadgade uppgifter. Det finns dock inga lagbestämmelser om befogenheter för underrättelseinhämtning. De civila myndigheternas informationsinhämtning baserar sig i huvudsak på brottsbekämpningsbefogenheter, offentliga källor och uppgifter som fås inom ramen för internationellt och annat frivilligt samarbete.

Myndigheterna inom inrikesministeriets förvaltningsområde, i synnerhet skyddspolisen, har en viktig roll när det gäller att avvärja hot av civil natur som riktas mot den nationella säkerheten. Skyddspolisen är en riksomfattande polisenhet som har till uppgift att bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet samt att utföra undersökning av sådana brott. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att förebygga verksamhet som äventyrar rikets säkerhet. Skyddspolisen bedriver inom sitt verksamhetsområde kontinuerlig säkerhetsunderrättelseinhämtning enligt sin uppgift och upprätthåller den nationella och internationella lägesbild av statens säkerhetspolitiska omgivning som uppkommer på detta sätt samt rapporterar om dessa till statsledningen och säkerhetsmyndigheterna.

Skyddspolisens informationsinhämtningsbefogenheter baserar sig på allmänna lagar om polisens verksamhet, i huvudsak på polislagen samt förundersökningslagen och tvångsmedelslagen. Utövandet av informationsinhämtningsbefogenheterna anknyter till förebyggande, avslöjande och utredning av brott samt i vissa fall till avvärjande av fara.

Försvarsmakten, som hör till försvarsministeriets förvaltningsområde, ansvarar för Finlands militära försvar. Militära underrättelseinhämtningsuppgifter hänför sig till bildandet och upprätthållandet av en militärstrategisk lägesbild samt säkerheten i samband internationella uppdrag. Det finns inga explicita lagbestämmelser om militär underrättelseinhämtning. Inom den militära försvarssektorn ansvarar försvarsmaktens militära kontraspionage, utan att begränsa skyddspolisens lagstadgade behörighet, för förebyggande av olaglig underrättelseverksamhet

som riktas mot Finland och för förhindrande av brott som äventyrar det militära försvarets syfte, dock inte för den relaterade brottsutredningen, som omfattas av skyddspolisens ansvar.

Den 13 december 2013 tillsatte försvarsministeriet en arbetsgrupp för att utveckla lagstiftningen för att förbättra säkerhetsmyndigheternas, i synnerhet skyddspolisens och försvarsmaktens, förmåga att inhämta information. Ett mål var att klarlägga lagstiftningsläget i fråga om behörighetsregleringen av säkerhetsmyndigheternas informationsinhämtning. Ett annat mål var att bedöma hur man bättre ska kunna värna om den nationella säkerheten i synnerhet för att avvärja hot som förekommer i datanäten.

Arbetsgruppen överlämnade sitt betänkande till försvarsministeriet den 14 januari 2015 (Riktlinjer för en finsk underrättelselagstiftning. Betänkande av arbetsgruppen för en informationsanskaffningslag). Arbetsgruppen föreslog att det skapas en rättsgrund för civil och militär underrättelseinhämtning. För detta syfte föreslog den att det inleds ett eller flera lagstiftningsprojekt som kan beredas inom olika ansvarsområden. I det sammanhanget bör det också övervägas om beredningen kunde vara exempelvis parlamentarisk eller annars ske under politisk styrning.

Arbetsgruppens betänkande sändes på remiss. Ett sammandrag över remissyttrandena publicerades den 30 juni 2015. Remissorganen ställde sig i regel bakom förslaget att utveckla lagstiftningen om underrättelseinhämtning.

Samtidigt med arbetsgruppen för en informationsanskaffningslag arbetade en arbetsgrupp som inrikesministeriet tillsatt för att utreda skyddspolisens administrativa ställning, resultatstyrning samt utveckling av övervakningen. Arbetsgruppen granskade delvis samma frågor som försvarsministeriets arbetsgrupp. Inrikesministeriets arbetsgrupp publicerade sin slutrapport den 24 september 2014 (Inrikesministeriets publikation 28/2014). I slutrapporten konstateras det att om skyddspolisens uppgifter och befogenheter utvecklas i en riktning som betonar underrättelseinhämtning, uppstår det ett behov att omarbeta formerna för den externa laglighetsövervakningen och den parlamentariska övervakningen. Alternativ som kan komma i fråga är exempelvis krav på nya domstolstillstånd eller inrättande av ett särskilt parlamentariskt tillsynsorgan. Om betydelsen av elementen i skyddspolisens underrättelseinhämtning som avser utländska förhållanden ökar ytterligare, bör utvecklingen av regleringen av uppgifterna och befogenheterna, styrningen och övervakningen inom den civila underrättelsen och den militära underrättelsen beakta varandra. Likaså gäller att om skyddspolisens befogenheter för underrättelseinhämtning utvidgas, bör man i syfte att säkerställa en rättvis rättegång överväga en begränsning av skyddspolisens förundersökningsuppgifter och förundersökningsbefogenheter. Skyddspolisen kan fortsättningsvis enligt behov delta i förundersökningar i egenskap av expertmyndighet.

Beredningen av underrättelselagstiftningen är förankrad i regeringsprogrammet. Enligt regeringsprogrammet för statsminister Juha Sipiläs regering kräver de ökande riskerna och nya hoten beredskap och förberedelser av ett nytt slag av hela samhället. I enlighet med regeringsprogrammet är målet att stärka det övergripande säkerhetstänkandet nationellt, inom Europeiska unionen och inom ramen för det internationella samarbetet. Detta gäller framför allt nya och omfattande hot som påverkansåtgärder av hybridkaraktär, cyberattacker och bekämpning av terrorism. I programmet föreslår regeringen att underrättelseinhämtning som avser utländska förhållanden och underrättelseinhämtning som avser datatrafik ska basera sig på lagstiftning. Genom lagstiftningen vill man bättre än förr kunna reagera på förändringarna i den säkerhetspolitiska omgivningen och nya hot som berör Finland. Samtidigt framhävs det att tillgodoseendet av de grundläggande fri- och rättigheterna och de mänskliga rättigheterna ska beaktas vid beredningen.

Inrikesministeriet inledde ett projekt för civil underrättelseinhämtning, försvarsministeriet inledde ett projekt för militär underrättelseinhämtning och justitieministeriet inledde ett projekt för eventuell ändring av grundlagen. Det bestämdes att projekten skulle beredas i nära samarbete mellan tre separata arbetsgrupper. Vidare konstaterades det att kommunikationsministeriet erbjuder arbetsgrupperna experthjälp när det gäller att beakta den digitala utvecklingen. Inrikesministeriet tillsatte också en parlamentarisk uppföljningsgrupp för projekten för reform av underrättelselagstiftningen. Uppföljningsgruppen skulle fungera som en länk mellan lagstiftningsprojekten och riksdagen för att riksdagen kontinuerligt ska vara medveten om hur projekten framskrider.

Inrikesministeriets projekt hade som mål att koncentrera sig på beredningen av lagstiftning om civil underrättelseinhämtning. Det viktigaste målet med projektet var att förbättra den nationella säkerheten. Målsättningen var att förbättra säkerhetsmyndigheternas förmåga att inom sitt ansvarsområde förutse och förebygga sådana skadliga gärningar och åtgärder som kan äventyra speciellt viktiga nationella intressen.

För närvarande finns det inga bestämmelser om särskilda befogenheter för skyddspolisen att inhämta information om hot mot statens säkerhet. Skyddspolisens viktigaste uppgift är att i samarbete framför allt med centralkriminalpolisen förebygga och avslöja förehavanden som är kopplade till terrorism, olaglig underrättelseverksamhet, spridning av massförstörelsevapen, extremiströrelser och till organiserad brottslighet som äventyrar statens säkerhet. I projektet övervägdes om befogenheterna bör utvecklas så att de omfattar personbaserad underrättelseinhämtning som avser utländska förhållanden och underrättelseinhämtning som avser utländska informationssystem samt underrättelseinhämtning som riktas mot den gränsöverskridande datatrafiken.

Målet var att bereda centrala bestämmelser om civil underrättelseinhämtning och på så vis förbättra skyddspolisens inhämtning av information om allvarliga internationella hot relaterade till polisens uppgifter så att skyddspolisen har befogenheter för personbaserad underrättelseinhämtning som avser utländska förhållanden och underrättelseinhämtning som avser utländska informationssystem samt för underrättelseinhämtning som avser datatrafik. Vid behov kan beredningen också genomföras stegvis med beaktande av de eventuella begränsningar som för närvarande följer av grundlagen. Bestämmelserna om den militära underrättelseinhämtningen och de bestämmelser om civil underrättelseinhämtning som samtidigt bereds vid inrikesministeriet bör vara sammanjämkade med varandra.

Den 17 oktober 2016 inledde justitieministeriet ett projekt för att bereda lagstiftning om övervakning av underrättelseverksamheten. Den 9 februari 2017 ändrades arbetsgruppens mandat till att gälla beredning av lagstiftning om ordnandet av laglighetskontroll av de civila och militära underrättelsemyndigheternas underrättelseverksamhet. Beredningen av lagstiftning om parlamentarisk kontroll överfördes till en intern arbetsgrupp vid riksdagens kansli tillsatt av riksdagens generalsekreterare.

Den 28 september 2015 tillsatte justitieministeriet en sakkunnigarbetsgrupp för att utreda och bereda en revision av grundlagsregleringen om skyddet för hemligheten i fråga om förtroliga meddelanden. Sakkunnigarbetsgruppen hade i uppdrag att för den parlamentariska beredning som tillsätts senare utreda och bereda en revision av grundlagen så att det för att trygga den nationella säkerheten genom lag kan föreskrivas om nödvändiga begränsningar i skyddet för förtroliga meddelanden, när de förutsättningar som ska anses vara behövliga är uppfyllda. Justitieministeriets förslag till en revision av grundlagen färdigställdes den 23 september 2016. Arbetsgruppen föreslog att 10 § i grundlagen ska ändras så att det till paragrafen fogas ett nytt 4 mom. där alla bestämmelser om förutsättningarna för begränsning av hemligheten i fråga om förtroliga meddelanden samlas. Genom lag kan enligt förslaget föreskrivas om sådana be-

gränsningar i meddelandehemligheten som är nödvändiga vid bekämpning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång, vid säkerhetskontroll och under frihetsberövande samt för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten.

2 Nuläge

2.1 Säkerhetsmiljön i förändring

Den 5 oktober 2017 godkände statsrådet ett principbeslut om strategin för den inre säkerheten. Strategin grundar sig på den redogörelse för den inre säkerheten som lämnades till riksdagen i maj 2016. Också enligt strategin har Finlands säkerhetsmiljö obestridligen blivit mer komplicerad. Nya utmaningar och uppgifter kräver lämplig prestationsförmåga av myndigheterna. Säkerhetsmyndigheternas kärnfunktioner och servicenivå måste vara tryggade. Förändringar i säkerhetsmiljön ska bemötas genom att säkerhetsmyndigheternas lägesbild och befogenheter moderniseras och myndigheternas kapacitet förbättras. I nuläget står samhällets möjligheter att reagera på hot mot den nationella säkerheten på ett betydande sätt i disproportion till de skador som uppstår om hoten förverkligas.

Hot uppstår i nya former, enligt strategin exempelvis i form av terrorism samt hybrid- och cyberhot, och dessa kan också fungera som medel i maktpolitiken. Målet är att inrikesministeriets och statsrådets övergripande lägesbild och den analyserade information som skaffats genom civil underrättelseinhämtning ska stå till förfogande i rätt tid för alla aktörer som deltar i skyddet av den nationella säkerheten. Målet är också att säkerhetsmyndigheternas beredskap och kapacitet ska förbättras enligt de krav som den förändrade omvärlden ställer genom att befogenheterna, beredskapen, handlingsmodellerna och resurserna utvecklas. Vidare stärks kompetensen inom säkerhetsaktörernas strategiska säkerhetskommunikation, och genom samarbete mellan myndigheter och andra aktörer minskas de negativa konsekvenser som avsiktlig och målinriktad spridning av felaktig information medför för säkerheten.

Den 19 maj 2016 lämnade statsrådet riksdagen en redogörelse för Finlands inre säkerhet (SRR 5/2016 rd) och den 17 juni 2016 en redogörelse för Finlands utrikes- och säkerhetspolitik (SRR 6/2016 rd). Båda redogörelserna baserar sig på begreppet övergripande säkerhet så som regeringsprogrammet förutsätter. Statsrådets försvarsredogörelse lämnades till riksdagen den 16 februari 2017. Den genomför den säkerhets- och försvarspolitiska redogörelsen. Redogörelsen för den inre säkerheten, den utrikes- och säkerhetspolitiska redogörelsen samt försvarsredogörelsen utgör en central referensram för den övergripande säkerheten. Bakgrunden till detta arbete utgjordes av 2012 års säkerhets- och försvarspolitiska redogörelse samt 2010 års säkerhetsstrategi för samhället.

Enligt redogörelsen för den inre säkerheten flyter hoten mot den inre och den yttre säkerheten allt mer in i varandra. Hoten kompliceras och förändras snabbt. Situationens förutsebarhet har försvagats betydligt under den senaste tiden, och i säkerhetssituationen finns ingen förbättring i sikte. I det nya läget har den inre säkerheten fått en framträdande betydelse, och därför sammanställde statsrådet för första gången en separat redogörelse för den inre säkerheten.

De försämrade relationerna mellan Ryssland och väst, den internationella terrorismen, cyberhoten och den omfattande olagliga migrationen är enligt redogörelsen för den inre säkerheten de viktigaste förändringarna i säkerhetsmiljön under den senaste tiden. Enligt redogörelsen har hybridmetoderna ökat i staters påverkan och måste myndigheterna som ansvarar för den inre säkerheten ha såväl förmåga att upptäcka hoten som tillräckliga resurser att hantera situationen, även då den blir långvarig. Man måste också identifiera och kunna reagera på staters och andra aktörers informationspåverkan. I det förändrade läget får det statliga beslutsfattandet

och säkrandet av de yttre gränsernas okränkbarhet en framträdande ställning. Även nya spänningar mellan stater är möjliga. Dessutom är de utländska underrättelsetjänsternas verksamhet i Finland tillbaka på samma nivå som under kalla kriget. Vid sidan av underrättelseverksamhet som bygger på personkällor bedrivs nu också underrättelseverksamhet i it-miljöer. Sabotage som skadar kritisk infrastruktur kan påverka en stor mängd människor. Exempelvis försörjningsberedskap, digitalisering, cybersäkerhet och grundläggande infrastruktur samt deras starka inbördesberoende är enligt redogörelsen centrala element i den inre säkerheten.

Enligt den utrikes- och säkerhetspolitiska redogörelsen fortsätter den kraftiga omvälvningen i den utrikes- och säkerhetspolitiska omvärlden såväl på Finlands närområden som globalt. Stater och andra aktörer har allt närmare och mångsidigare förbindelser till varandra och är beroende av varandra. Den senaste omvälvningen i omvärlden har också skapat nya hot och instabilitet. Den internationella säkerhetssituationen har ur ett europeiskt perspektiv försämrats under de senaste åren. Förändringarna i den utrikes- och säkerhetspolitiska omvärlden har många slags konsekvenser även för Finlands interna utveckling. Den inre säkerheten utsätts därmed för nya osäkerhetsfaktorer och samhällets allmänna kristålighet sätts på prov.

Enligt den utrikes- och säkerhetspolitiska redogörelsen bygger den utrikes- och säkerhetspolitiska måluppställningen, beslutsfattandet och påverkan på kunskap om omvärlden. Det är viktigt att kontinuerligt samla in och analysera information om variabler i omvärlden och om de möjligheter och hot som de ger upphov till. Det måste finnas beredskap att anpassa verksamheten och vid behov prioriteringarna i utrikes- och säkerhetspolitiken utifrån information och analys. De viktigaste yttre variablerna i Finlands utrikes- och säkerhetspolitiska omvärld är de globala utvecklingstrenderna, den politiska utvecklingen och säkerhetsutvecklingen på för Finland viktiga geografiska områden, utrikes- och säkerhetspolitiska aktörer samt internationella regler. De redogörelser som nämns ovan betonar vikten av att förbättra finländarnas säkerhet och välfärd. Bekämpning av och beredskap inför gränsöverskridande hot kräver att både civila och militära resurser utnyttjas, att ett brett urval av verktyg används. Finland måste utifrån sina egna styrkor kunna förutse förändringar i omvärlden och bemöta de krav som förändringarna ställer. En situation där Finlands myndigheter på grund av bristfällig nationell reglering är beroende av andra länder för att få information om hot mot Finlands livsviktiga intressen är enligt redogörelsen för den inre säkerheten ohållbar. Varje stat – även Finland – har skyldighet att sörja för sin egen och sina medborgares säkerhet och bygga beslutsfattandet om detta på självförvärvad information.

Statsrådets försvarsredogörelse bekräftar att säkerhetsläget i Finlands närområden har blivit sämre och konstaterar att spänningarna i Östersjöområdet och osäkerheten i sig även mera vidsträckt har ökat ytterligare. Vid sidan om militära maktmedel kan man också använda annan omfattande metodarsenal för att uppnå målen.

I de redogörelser som nämns ovan får s.k. hybridpåverkan en synlig position. Hybridpåverkan kan definieras som planmässig verksamhet, där en stat eller en icke-statlig aktör samtidigt drar nytta av en rad militära medel eller t.ex. ekonomiska eller teknikbaserade påtryckningsmedel, informationsoperationer och sociala medier i sin strävan att dra nytta av målstatens sårbarheter. Påverkan kan inriktas på såväl politiska, ekonomiska och militära strukturer som infrastrukturen i målstaten. Hybridpåverkan handlar vanligtvis inte om åtgärder som förbereder ett väpnat anfall, utan om sådana påtryckningsåtgärder som är så effektiva att det inte behövs något väpnat anfall.

Digitaliseringens inverkan på utvecklingen i säkerhetsmiljön

Digitaliseringens inverkan på utvecklingen i säkerhetsmiljön samt cybersäkerhet behandlas bl.a. i strategin för cybersäkerheten i Finland (statsrådets principbeslut av den 24 januari 2013)

och i försvarsministeriets betänkande Riktlinjer för en finsk underrättelselagstiftning (betänkande av arbetsgruppen för en informationsanskaffningslag) från 2015.

Cybersäkerhetsstrategin konstaterar att Finland i egenskap av ett informationssamhälle är beroende av att datanäten och informationssystemen fungerar och därmed också är mycket sårbart för störningar som riktas mot dem. De hot som riktar sig mot cyberomgivningen har förändrats så att konsekvenserna av dem har blivit allt farligare för enskilda människor, företag och hela samhället. De aktörer som åstadkommer dessa hot är mera professionella än tidigare, och numera kan också statliga aktörer räknas till dem. Attacker som genomförs i cyberomgivningen kan användas som verktyg för politisk och ekonomisk påtryckning och i en allvarlig kris som en påverkningsmetod utöver traditionella militära maktmedel.

Betänkandet av arbetsgruppen för en informationsanskaffningslag tar upp digitaliseringens konsekvenser ur perspektivet för både kommunikation och hot som riktas mot datanät. Ur ett kommunikationsperspektiv innebär digitaliseringen att aktörer som hotar den nationella säkerheten kan nätverka på betydligt mer omfattande och varierande sätt än tidigare. Bland dessa aktörer används datanäten som ett verktyg för att informera om planer och avsikter som gäller gärningar som genomförs i realvärlden. Gärningarna kan vara militära (väpnat anfall) eller riktas mot andra nationella intressen än statens territoriella integritet (spionage, terrordåd, export av varor med dubbla användningsområden). Datanät används också som egentliga redskap för att utsätta objektet – exempelvis finska staten – för gärningar som allvarligt skadar det. Det kan handla om i strategin för cybersäkerheten i Finland avsedda gärningar som karaktäriseras som cyberspionage eller cyberterrorism.

Enligt bedömning från säkerhetsmyndigheterna försöker flera främmande makter rikta omfattande och tekniskt avancerat cyberspionage mot den finska statsförvaltningen och de företag som är av samhällsekonomisk betydelse. Vid cyberspionage används inte vanliga sabotageprogram som kan upptäckas med kommersiella antivirusprogram, utan tekniskt avancerade och mångsidiga verktyg för nätattacker. Spionageoperationerna har planerats noggrant på förhand och har ett exakt operativt syfte att samla information om exempelvis omständigheter som är förknippade med målstatens utrikes- och säkerhetspolitik, ekonomi och industri. Som exempel på en spionageoperation av detta slag kan nämnas det angrepp som riktades mot utrikesministeriet och uppdagades hösten 2013. Utöver underrättelseprogram kan även informationssystem utsättas för sabotageprogram som aktiveras när en kris börjar.

Enligt betänkandet av arbetsgruppen för en informationsanskaffningslag kommer cyberspionage och cyberoperationer att få allt större betydelse under de kommande åren. Skälen till detta är möjligheten att genomföra dåd i cyberomgivningen till låga kostnader, svårigheten och de höga kostnaderna för att skydda sig samt de små riskerna att åka fast. Alla de främmande makter som är väsentliga med tanke på hur Finlands säkerhetspolitiska omgivning utvecklas satsar målmedvetet och ansenligt på att bygga upp sin offensiva cyberkapacitet. Som exempel på cyberoperationer som riktats mot stater kan nämnas nätattacker mot slutna myndighetsnät i Ukraina (2014), Georgien (2008) och Estland (2007). Dessa operationer visade sig vara välorganiserade och välplanerade, och det bedömdes att bakom dem stod en statsaktör eller parter som var mycket nära kopplade till en stat. I betänkandet av arbetsgruppen för en informationsanskaffningslag bedöms hotet om cyberattacker som genomförs i terroristiskt syfte mot Finland fortfarande vara begränsat, men i betänkandet påpekas att situationen kan förändras snabbt som en följd av utvecklingen i den internationella omvärlden. Tänkbara tillvägagångssätt för terroristgrupper utgörs av överbelastningsattacker, som skadar tillgången på kritiska nättjänster, samt sabotage via kontrollrumssystemet SCADA, vilket i värsta fall kan orsaka omfattande person- och egendomsskador.

Den 17 februari 2017 publicerade statsrådets kansli en obunden undersökning om cybersäkerhetsläget i Finland (Publikationsserie för statsrådets utrednings- och forskningsverksamhet 30/2017). Enligt undersökningen är den nationella observationsförmågan bristfällig när det gäller cybersäkerhetsincidenter. Därför är lägesmedvetenheten svag och förutsättningarna för att förhindra, begränsa och återhämta sig från allvarliga cyberattacker begränsade. Alla vitala funktioner i det finländska samhället och ur försörjningsberedskapssynvinkel kritiska företag är inte för närvarande tillräckligt väl skyddade mot olika slags cyberhot och även resiliensen (tåligheten) vad gäller störningssituationer är fortfarande på en svag nivå för en del av de objekt som bör skyddas. Man har inte lyckats uppdatera lagstiftningen i Finland i överensstämmelse med cybersäkerhetskraven. För en bättre observationsförmåga är det nödvändigt att revidera underrättelselagstiftningen.

2.2 Lagstiftning och praxis

Myndighetsfältet för den nationella säkerheten

Många olika statliga myndigheters verksamhet är av betydelse när det gäller att förutse och förbereda sig på förändringar i säkerhetsmiljön. Trots att det i det föregående har konstaterats att militära och civila hot allt mer flyter in i varandra, kan det alltjämt anses vara ändamålsenligt med en grundläggande indelning av dem. Försvarsmakten ansvarar för beredskapen inför och avvärjningen av militära hot. Försvarsmaktens uppgifter och befogenheter och den militära underrättelseverksamhetens uppgifter och befogenheter som en del av den behandlas i försvarsministeriet proposition om militär underrättelseverksamhet, vilken har samband med denna proposition.

Fältet av behöriga myndigheter är mera mångfasetterat när det gäller att förbereda sig på icke-militära hot. Det är inte ändamålsenligt eller ens möjligt att här behandla alla myndigheter vilkas uppgifter har betydelse för eller tangerar arbetet för att skydda den nationella säkerheten.

Polisen är den viktigaste ansvariga myndigheten med tanke på den inre säkerheten. Polisens uppgift är att trygga rätts- och samhällsskicket, upprätthålla allmän ordning och säkerhet samt förebygga, avslöja och utreda brott och föra brott till åtalsprövning. Inom polisorganisationen, som leds av Polisstyrelsen, har både centralkriminalpolisen som en riksomfattande enhet och de lokala polisinrättningarna uppgifter som anknyter till den nationella säkerheten.

Enligt 9 § i polisförvaltningslagen ska centralkriminalpolisen bekämpa internationell, organiserad, yrkesmässig, ekonomisk och annan allvarlig brottslighet. Centralkriminalpolisen ska bl.a. i regel utföra förundersökning av terroristbrott. Centralkriminalpolisen utför också undersökning av andra brott av relevans för den nationella säkerheten än sådana lands- och högförräderibrott som särskilt ålagts skyddspolisen. Vid centralkriminalpolisen finns den s.k. PTG-centralen, där polisen, gränsbevakningsväsendet och Tullen bedriver gemensam kriminalunderrättelse- och analysverksamhet. Syftet med verksamheten är att upprätthålla en lägesbild över brottsligheten, förbereda bekämpningsobjekt inom allvarlig gränsöverskridande och organiserad brottslighet, sammanlänka brott samt bereda kriminalunderrättelsepromemorior och hotbildsbedömningar. I anslutning till centralkriminalpolisen finns också Centralen för bekämpning av cyberbrott, som inrättades 2015.

I den lokala polisens uppgifter ingår utöver att förebygga, avslöja och utreda brott och föra brott till åtalsprövning också att upprätthålla allmän ordning och säkerhet. Den sistnämnda uppgiften omfattar bl.a. insatser för att på det lokala planet samordna verksamheten för förebyggande av och tidigt ingripande i våldsinriktad radikalisering.

Den riksomfattande enheten skyddspolisen separerades från den övriga polisorganisationen den 1 januari 2016. Denna proposition berör i väsentlig grad utvecklandet av skyddspolisens befogenheter, och därför behandlas skyddspolisens uppgifter närmare längre fram.

Övervakningen av Finlands yttre gränser och gränssäkerheten har betydelse för den nationella säkerheten och statssuveräniteten. Gränsbevakningsväsendet ansvarar för upprätthållandet av dessa, och bestämmelser om dess uppgifter finns i gränsbevakningslagen (578/2005). Även Tullen är behörig myndighet vid gränsövergångsställen, och enligt lagen om Tullens organisation (960/2012) ansvarar Tullen för bl.a. tullövervakningen av utlandstrafiken. Både gränsbevakningsväsendet och Tullen ska förhindra, avslöja och utreda brott i anslutning till sina egna uppgifter.

Migrationsverket (Migri) behandlar och avgör ärenden som gäller inresa, vistelse i landet, flyktingskap och finskt medborgarskap. För bedömningen av förutsättningarna för utlänningars inresa och vistelse i landet är det av betydelse att utlänningarnas verksamhet inte äventyrar den nationella säkerheten.

När den nationella säkerhetsmiljön förändras i snabb takt accentueras betydelsen av tidsenlig lägesinformation. Vid statsrådets kansli finns statsrådets lägescentral, som tar fram information om säkerhetsincidenter i realtid och sammanställer en lägesbild på basis av uppgifterna från de behöriga myndigheterna. Lägescentralen sammanför uppgifterna från de olika myndigheterna och från öppna källor och lämnar utifrån dessa en rapport till statsledningen och de olika myndigheterna. Lägescentralen är också Finlands nationella kontaktpunkt bl.a. gentemot Europeiska unionen på det sätt som anges särskilt. Bestämmelser om statsrådets lägescentrals uppgifter finns i lagen om statsrådets lägescentral (300/2017).

I och med internationaliseringen av den säkerhetspolitiska omgivningen har det blivit allt viktigare att erhålla information om utländska förhållanden. Enligt 13 § i reglementet för statsrådet (262/2003) hör utrikes- och säkerhetspolitiken, utrikespolitiskt betydelsefulla internationella ärenden samt de internationella relationerna i allmänhet till utrikesministeriets ansvarsområde. De beskickningar som hör till utrikesrepresentationen är verksamma under ledning och övervakning av utrikesministeriet. I beskickningarnas uppgifter enligt lagen om utrikesförvaltningen (204/2000) ingår att representera finska staten och bevaka Finlands politiska och övriga intressen. För fullgörandet av sina uppgifter samlar beskickningarna inom utrikesrepresentationen in uppgifter om stationeringsländerna och förhållanden i dem. Utöver andra uppgifter samlar utrikesförvaltningen in uppgifter om säkerhetsläget i främmande länder för det system för resemeddelanden som utrikesförvaltningen förvaltar. Det finns inte några nationella bestämmelser om beskickningarnas metoder för att fullgöra informationsinsamlingsuppgifterna. Den rättsliga ramen för verksamheten utgörs av internationella avtal som är bindande för Finland (Wienkonventionen om diplomatiska förbindelser (FördrS 3–5/1970) och Wienkonventionen om konsulära förbindelser (FördrS 49 och 50/1980)).

Inom kommunikationsministeriets förvaltningsområde finns Kommunikationsverket, vars uppgifter anges i lagen om kommunikationsförvaltningen (625/2001). Genom ett principbeslut av statsrådet inrättades ett cybersäkerhetscenter vid Kommunikationsverket vid ingången av 2014. Via Cybersäkerhetscentret producerar Kommunikationsverket informationssäkerhetstjänster för hela samhället och främjar Finlands beredskap inför cyberhot och hanteringen av de störningssituationer som de förorsakar. I Cybersäkerhetscentrets uppgifter ingår att upptäcka och utreda hot mot och kränkningar av informationssäkerheten samt att upprätthålla en lägesbild över cybersäkerheten. HAVARO är ett system som riktar sig till aktörer som är kritiska med tanke på försörjningsberedskapen och till statsförvaltningen och vars syfte är att upptäcka och varna för kränkningar av informationssäkerheten. Avsikten är att systemet ska producera information om kränkningar av informationssäkerheten för att organisationerna ska

kunna skydda sig mot kränkningarna och i förekommande fall begränsa de skador som kränkningarna orsakar. Kommunikationsverket svarar för HAVARO-systemet. Systemet har utformats i samarbete med Försörjningsberedskapscentralen. För aktörer inom statsförvaltningen tillhandahåller Kommunikationsverket också tjänsten GovHAVARO.

Uppgifterna för de myndigheter som behandlats i det föregående omfattas i vid bemärkelse av området för den nationella säkerheten. Upprätthållande av den nationella säkerheten eller inhämtande av information om hot mot den nationella säkerheten kan dock inte anses utgöra kärnan i deras uppgifter. Betänkandet av arbetsgruppen för en informationsanskaffningslag fastställde skyddspolisen som civil myndighet för den nationella säkerheten. Skyddande av den nationella säkerheten utgör kärnan i skyddspolisens lagstadgade uppgifter. Ett centralt mål med denna proposition är att för skyddande av den nationella säkerheten skapa en rättsgrund för skyddspolisens befogenheter för underrättelseinhämtning.

Skyddspolisens uppgifter

Skyddspolisen är en riksomfattande polisenhet under inrikesministeriet, och enligt 10 § (860/2015) 1 mom. i polisförvaltningslagen har skyddspolisen till uppgift att i enlighet med inrikesministeriets styrning bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet samt att utföra undersökning av sådana brott. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att förebygga verksamhet som äventyrar rikets säkerhet. I 2 mom. sägs att efter att ha hört Polisstyrelsen bestämmer inrikesministeriet närmare vilka kategorier av ärenden som ska undersökas av skyddspolisen och att efter att ha hört Polisstyrelsen bestämmer inrikesministeriet vid behov om samverkan och samarbetet mellan skyddspolisen och övriga polisenheter och om undersökningsarrangemangen i förhållandet mellan dem. Skyddspolisens verksamhetsområde fastställs i 10 § i polisförvaltningslagen genom en uppräkning av de skyddsobjekt – den inre säkerheten, den yttre säkerheten, statsskicket och samhällsskicket – som skyddspolisen ska skydda. I lagen nämns inga konkreta företeelser eller säkerhetshot som skyddspolisen ska bekämpa. Genom att definiera uppgifterna med utgångspunkt i skyddsobjekt har man uppenbarligen velat säkerställa att skyddspolisens verksamhet för att skydda statens centrala säkerhetsintressen kan anpassas till förändrade förhållanden samt att ämbetsverkets verksamhetsområde gällande bekämpningen är generellt. Den viktigaste uppgiften för skyddspolisen är att producera analyserad information om hot mot statens centrala säkerhetsintressen. För att fullgöra uppgiften producerar skyddspolisen strategisk information om olika fenomen och om omvärlden för säkerhetsmyndigheterna och som underlag för den högsta statsledningens säkerhetspolitiska beslutsfattande.

För att avvärja och avslöja hot mot den nationella säkerheten bedriver skyddspolisen informationsinhämtning, där den inhämtar behövlig information, ordnar den så att den blir användbar, analyserar den och rapporterar om den eller vidtar andra nödvändiga åtgärder. Informationen fås från öppna källor, genom egen operativ verksamhet, av nationella samarbetspartner och av utländska säkerhets- och underrättelsemyndigheter. För fullgörandet av de uppgifter som ämbetsverket har krävs det att skyddspolisen aktivt och på bred basis ger akt på Finlands säkerhetspolitiska omvärld och inhämtar information proaktivt.

Skyddspolisen har också uppgifter som anges i andra lagar, exempelvis i säkerhetsutredningslagen (726/2014) och i utlänningslagen (301/2004).

Enligt inrikesministeriets gällande föreskrift (SMDno-2015-2080) har skyddspolisen bl.a. följande uppgifter:

- Skyddspolisen producerar för säkerhetsmyndigheterna och den högsta statsledningens beslutsfattande strategisk information om Finlands säkerhetspolitiska omgivning och fenomen som är förknippade med den. Uppgiften fullgörs genom säkerhetsunderrättelseverksamhet och upprätthållande av en aktuell nationell och internationell lägesbild samt analyser av och rapporter till säkerhetsmyndigheterna om väsentliga observationer inom verksamhetsområdet. Uppgiften har karaktär av underrättelseinhämtning, och för fullgörandet krävs det att skyddspolisen aktivt och på bred basis ger akt på Finlands säkerhetspolitiska omvärld och inhämtar information proaktivt. Skyddspolisen producerar analyserad information som är nödvändig för förebyggande av hot mot statens centrala säkerhetsintressen.

- Skyddspolisen lämnar årligen inrikesministeriet ett förslag till prioriteter för skyddspolisens informationsinhämtning och vid behov ett förslag till ändringar i prioriteterna.

- Skyddspolisens operativa huvuduppgifter går ut på att bekämpa terrorism samt följa främmande makters underrättelseverksamhet och bekämpa, förebygga och avslöja för Finland skadliga konsekvenser av den.

- Skyddspolisen samarbetar med olika myndigheter för att förhindra spridning av massförstörelsevapen.

- Skyddspolisen bekämpar, förebygger och avslöjar våldsinriktad radikalisering och illegal extremism som hänför sig till statens inre säkerhet samt ger akt på de hot som organiserad brottslighet medför för den nationella säkerheten och tar för sitt verksamhetsområde del i den riksomfattande lägesbild som Centralkriminalpolisen upprätthåller över helhetsbrottsligheten och den allvarliga brottsligheten samt bekämpningsläget.

- Skyddspolisen gör i förekommande fall hotbildsbedömningar i anslutning till statsbesök och storskaliga möten och deltar i säkerhetsplaneringen inför besöken och mötena.

- Skyddspolisen ansvarar för analys av statens säkerhetspolitiska omgivning inom sitt verksamhetsområde samt upprätthåller verksamhetsområdets nationella och internationella lägesbild och ser till att lägesbilder med hotbildsbedömningar förmedlas till inrikesministeriet, Polisstyrelsen, polisenheterna och övriga berörda myndigheter.

- Skyddspolisen rapporterar till statsledningen om centrala angelägenheter inom sitt verksamhetsområde. Skyddspolisen tar också del i utformningen av statsledningens säkerhetslägesbild.

- Skyddspolisen utför förebyggande säkerhetsarbete som hänför sig till dess verksamhetsområde genom styrning och rådgivning för myndigheter och privata sammanslutningar samt genom säkerhetsutredningar av personer och säkerhetsutredningar av företag.

- Skyddspolisen ger utlåtanden om i synnerhet utlänningars inresa, deras vistelse i landet och beviljande av medborgarskap samt om andra ärenden som hänför sig till dess verksamhetsområde.

- Inom polisförvaltningen svarar skyddspolisen för förhindrande, avslöjande och även utredning av brott som avses i 12 kap. (landsförräderibrott) och 13 kap. (högförräderibrott) i strafflagen. Skyddspolisen svarar för förundersökningen också när brott som avses i strafflagens 17 kap. 1 § (offentlig uppmaning till brott), 15 kap. 10 § 1 mom. (underlåtenhet att anmäla grovt brott) eller 15 kap. 11 § (skyddande av brottsling) anknyter till landsförräderibrott eller högförräderibrott.

- När det gäller terroristbrott som avses i 34 a kap. i strafflagen går skyddspolisens uppgift ut på att förhindra och avslöja sådana brott. Förundersökning av terroristbrott utförs vid en polisenhet under Polisstyrelsen, och skyddspolisen samarbetar med enheten och bistår vid förundersökningen när det behövs. Av särskilda skäl som hänför sig till statens säkerhet kan skyddspolisen utföra förundersökning av brott som gäller terrorism på det sätt som överenskommits med skyddspolisen och Polisstyrelsen.

- Skyddspolisen bistår och samarbetar med förundersökningsenheten också vid förundersökning av andra brott av betydelse för Finlands inre och yttre säkerhet än sådana brott som nämns ovan. Gärningar som nämns i 11 och 14 kap. i strafflagen är exempel på sådana brott.

Enligt 4 a § i polisförvaltningslagen ska skyddspolisen underrätta inrikesministern om sådana angelägenheter i skyddspolisens uppgifter som är av samhällelig betydelse, och dessutom underrätta polisöverdirektören om dessa angelägenheter, om de har betydande inverkan på det övriga polisväsendet. Enligt motiveringen till bestämmelsen är skyddspolisen skyldig att informera även republikens president, statsministern och utrikesministern med beaktande av de utrikes- och säkerhetspolitiska uppgifter som föreskrivits för dem. Dessutom informerar skyddspolisen riksdagens grundlags-, förvaltnings- och utrikesutskott om utvecklingen av säkerhetsläget i Finland.

För skötseln av skyddspolisens förebyggande uppgift preciseras anmälningsskyldigheten i polisförvaltningsförordningen (158/1996). Enligt 8 § i förordningen ska skyddspolisen, för att fullgöra sin lagstadgade uppgift, meddela myndigheter och sammanslutningar sådana anvisningar, råd och upplysningar som behövs för upprätthållande av den nationella säkerheten eller för att förhindra att den kränks.

Skyddspolisens informationsinhämtning

Skyddspolisens viktigaste uppgift är att förebygga och avslöja brott och förehavanden som är kopplade till terrorism, olaglig underrättelseverksamhet, spridning av massförstörelsevapen och extremiströrelser. En förutsättning för att uppgiften ska kunna fullgöras är att skyddspolisen kan inhämta information om brott och förehavanden av detta slag.

För inhämtande av offentligt tillgänglig information krävs det inte någon särskilt föreskriven myndighetsbehörighet som grund. Eftersom strävan är att de förehavanden och brott som skyddspolisen ska bekämpa förbereds i hemlighet, kan man i praktiken inte grunda informationsinhämtningen på den information som finns att tillgå offentligt. Därför måste skyddspolisen till centrala delar få information om verksamhet som bedrivs i hemlighet. För att vara effektivt måste inhämtandet av information dessutom utföras i hemlighet för dem som åtgärden riktas mot.

Det finns inte några bestämmelser om särskilda befogenheter för skyddspolisen att inhämta information om hot mot statens säkerhet. Skyddspolisen är en polismyndighet som i sin verksamhet använder sig av de brottsbekämpningsrelaterade befogenheter för informationsinhämtning och andra befogenheter som har föreskrivits för polisen.

De hemliga metoder för inhämtande av information för att förhindra och avslöja brott som föreskrivs i polislagen är viktiga i skyddspolisens praktiska verksamhet. För skyddspolisens del begränsas brottsutredningsuppgifterna i praktiken främst till undersökning av spioneribrott. Skyddspolisen utför endast sällan förundersökning.

Polisrättsliga principer

I 1 kap. i polislagen finns bestämmelser om s.k. polisrättsliga principer: respekt för de grundläggande rättigheterna och de mänskliga rättigheterna (2 §), proportionalitetsprincipen (3 §), principen om minsta olägenhet (4 §) och principen om ändamålsbundenhet (5 §) samt åtgärdseftergift och åtgärdsfördröjning (9 §). Principerna för verksamheten har angetts på ett allmänt plan och gäller skötseln av alla polisuppgifter och all utövning av polisbefogenheter. Principerna är generella, men framgår indirekt på nytt också av ordalydelsen i flera enskilda bestämmelser i polislagen. Vikten av att följa principerna framhävs i samband med användning av maktmedel och i samband med hemliga metoder för inhämtande av information samt även allmänt i samband med att polisåtgärder innebär väsentligt ingripande i medborgarnas rättssfär.

Enligt bestämmelsen om respekt för de grundläggande rättigheterna och de mänskliga rättigheterna i 1 kap. 2 § i polislagen gäller att när polisen utövar sina befogenheter ska den välja det alternativ som bäst och med minsta olägenhet tillgodoser dessa rättigheter.

Med proportionalitetsprincipen avses att de medel som tillämpas och de olägenheter som de medför ska stå i rimlig proportion till det mål som eftersträvas. Proportionalitetsprincipen uttrycks i 1 kap. 3 § i polislagen, och paragrafen lyder som följer: ”Polisens åtgärder ska kunna försvaras i förhållande till hur viktigt, farligt och brådskande dess uppdrag är, det mål som eftersträvas samt uppträdande, ålder, hälsa och andra motsvarande omständigheter som gäller den person som är föremål för åtgärden och övriga omständigheter som inverkar på helhetsbedömningen av situationen.”

En specialbestämmelse som uttrycker tankegången i proportionalitetsprincipen finns också i 1 kap. 9 § i polislagen med rubriken ”Åtgärdseftergift och åtgärdsfördröjning”. Enligt bestämmelsen har polisen rätt att avstå från en åtgärd om slutförandet av den kunde leda till ett oskäligt slutresultat i förhållande till det mål som eftersträvas. Det är meningen att bestämmelsen ska förhindra uppkomsten av sådana situationer där utövandet av polisbefogenheter kan orsaka den som saken gäller eller utomstående personer större olägenhet än den rättskränkning eller den störning som man avser att avvärja.

Principen om minsta olägenhet uttrycker vikten av att uppfylla kravet på att åtgärderna ska vara nödvändiga. Tidigare talades det allmänt om principen om nödvändighet. Polisens åtgärder ska genomföras så att de inte ingriper i någons rättigheter i större utsträckning och inte orsakar någon större skada eller olägenhet än vad som är nödvändigt för att utföra uppdraget. När polisen bedömer om åtgärderna behövs är utgångspunkten att den får göra bedömningen bara i förhållande till möjligheten att nå de mål som polisen eftersträvar. När det gäller tillämpning av behörighetssystemet är det således inte möjligt att tänka på samhällets ”allmänna fördel” vid utförandet av polisuppgifter.

I polisarbetet får inte utövas makt i större utsträckning än situationen nödvändigt kräver. I samband med polisuppgifter är det ofta möjligt att överväga olika åtgärder för att lösa situationen. Valet styrs av kravet på nödvändighet. Det gäller att välja den metod som innebär att olägenheten blir så liten som möjligt. Det kan i praktiken betyda att polisen inte kan välja det tillvägagångssätt som passar den bäst eller som är det behändigaste och billigaste. Principens praktiska betydelse framgår kanske tydligast i de situationer där polisen är tvungen att överväga att använda olika typer av maktmedel eller hemliga metoder för inhämtande av information.

Kravet på nödvändighet framgår också på så vis att endast sådan utövning av makt är berättigad som bidrar till det resultat som polisen eftersträvar. Exempelvis telefonavlyssning får inte

riktas mot en person trots att det till synes finns förutsättningar för teleavlyssning, om det med tanke på situationen är känt att det faktiska målet ändå inte kommer att nås genom teleavlyssning. Det att principen om nödvändighet blir bortglömd innebär då att polisåtgärden omvandlas till ogrundat ingripande i de grundläggande rättigheterna och de mänskliga rättigheterna.

Polisen kan i sin verksamhet bli tvungen att ingripa kraftfullt och till och med mycket konkret i den rättsliga ställningen för den person som är föremål för åtgärden. Det här understryker vikten av att kravet på ovillkorlig lagenlighet uppfylls i alla polisuppgifter. De högsta laglighetsövervakarna har i sin avgörandepraxis ibland varit tvungna att fästa uppmärksamhet vid att i samband med varje uppgift som polisen har gäller att polisen får utöva sina befogenheter endast för ändamål som explicit gäller den aktuella uppgiften. Det är således inte tillåtet att utöva makt för att till synes utföra en uppgift för vilken maktutövning i sig kan vara lämplig, om det faktiska målet trots allt är att skapa behörighet för en helt annan åtgärd till vilken det inte alls finns någon rätt att koppla de aktuella befogenheterna. Enligt 1 kap. 5 § i polislagen får polisen utöva sina befogenheter endast i föreskrivna syften.

Förutsättningar för användning av hemliga metoder för inhämtande av information

Med förhindrande av brott avses enligt 5 kap. 1 § 2 mom. i polislagen åtgärder som syftar till att förhindra brott, försök till brott och förberedelse till brott, när det utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet finns grundad anledning att anta att personen i fråga kommer att göra sig skyldig till brott, samt åtgärder som syftar till att avbryta ett redan påbörjat brott eller begränsa den direkta skada eller fara som brottet medför. Med uttrycket ”utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet” avses direkta iakttagelser av en persons egen verksamhet och av en utomstående person, t.ex. tips från en informationskälla, och annan indirekt utredning. Information som fåtts genom iakttagelser och annan information omfattar också bl.a. information som fåtts genom förfrågningar, observationer och antydningar/tips samt slutsatser på basis av brottsanalyser. En förutsättning för användning av en föreskriven metod för inhämtande av information för förhindrande av brott är att det på basis av denna information med fog kan antas att en person gjort sig skyldig till brott (RP 224/2010 rd, s. 93).

Förhindrande av brott enligt polislagen är förebyggande myndighetsverksamhet i en tidig fas. Enligt 5 kap. 1 § 2 mom. i polislagen omfattar förhindrande av brott åtgärder som syftar till att förhindra försök till brott och förberedelse till brott. Med förhindrande av förberedelse avses förhindrande av förberedelse till en straffbar gärning även då själva förberedelsen inte har kriminaliserats.

Med avslöjande av brott avses enligt 5 kap. 1 § 3 mom. i polislagen åtgärder som syftar till att klarlägga om det för inledande av förundersökning finns en i 3 kap. 3 § 1 mom. i förundersökningslagen avsedd grund, när det utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet kan antas att ett brott har begåtts. Begreppet avslöjande av brott avser gråzonen mellan förhindrande respektive utredning av brott. Det är inte fråga om brottsutredning eftersom förutsättningar för inledande av förundersökning saknas, men inte heller förhindrande av brott, eftersom brottet redan antas ha blivit begånget. Som exempel kan nämnas en situation där man fått tips om att ett brott redan har begåtts men där det inte finns någon konkret grund för misstanken och inte heller någon sådan orsak att misstänka brott som avses i förundersökningslagen. (RP 224/2010 rd, s. 93).

I 5 kap. i polislagen ingår bestämmelser om sådana hemliga metoder för inhämtande av information som skyddspolisen får använda för att inhämta information i hemlighet för dem som de riktas mot. Hemliga metoder för inhämtande av information är teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teleövervakning med samtycke av

den som innehar teleadress eller teleterminalutrustning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, teknisk spårning, teknisk observation av utrustning, inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp, användning av informationskällor och styrd användning av informationskällor samt kontrollerade leveranser.

De hemliga metoderna för inhämtande av information kan grupperas på olika sätt enligt användningssätt och syfte. Teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teleövervakning med samtycke av den som innehar teleadress eller teleterminalutrustning samt teknisk avlyssning är tekniska metoder för inhämtande av information som riktas mot målpersonens kommunikation. Användning av informationskällor och styrd användning av informationskällor som hänför sig till den betraktas som traditionella metoder för inhämtande av information om en person. Vid användning av informationskällor inhämtas information om målpersonen via mellanhänder. Förtäckt inhämtande av information, täckoperationer och bevisprovokation genom köp är sådana metoder för inhämtande av information om en person som genomförs i växelverkan mellan den som använder metoden å ena sidan och en mellanhand eller målpersonen direkt å andra sidan och som innebär att målpersonen förs bakom ljuset. Teknisk avlyssning, optisk observation, teknisk spårning och teknisk observation av utrustning är metoder för tekniska iakttagelser av målpersonens beteende. Systematisk observation baserar sig i sin tur på iakttagelser av målpersonens beteende utgående från sinnesintryck.

En allmän förutsättning för användning av en hemlig metod för inhämtande av information är enligt 5 kap. 2 § 1 mom. i polislagen att man med den metoden kan antas få information som behövs för förhindrande, avslöjande eller avvärjande av risk för brott. I fråga om teleavlyssning, inhämtande av information i stället för teleavlyssning, systematisk observation, teknisk avlyssning, teknisk spårning av personer, teknisk observation av utrustning, täckoperationer, bevisprovokation genom köp, styrd användning av informationskällor och kontrollerade leveranser innehåller 2 mom. i samma paragraf en tilläggsförutsättning enligt vilken metoderna får användas bara om de kan antas vara av synnerlig vikt för förhindrande eller avslöjande av ett brott. För täckoperationer och bevisprovokation genom köp förutsätts dessutom att metoden är nödvändig för att ett brott ska kunna förhindras eller avslöjas.

För användningen av olika metoder för inhämtande av information har i polislagen ställts s.k. allmänna förutsättningar och särskilda förutsättningar. Särskilda förutsättningar för användningen av hemliga metoder för inhämtande av information är framför allt de specificerade brott, för vilkas förhindrande varje metod kan användas. I bestämmelserna om de olika metoderna för inhämtande av information kan det också ställas andra särskilda förutsättningar. Sammanfattande kan konstateras att skyddspolisen på ett heltäckande sätt kan använda de hemliga metoder för inhämtande av information som anges i 5 kap. i polislagen för att förhindra terroristbrott som är straffbara enligt 34 a kap. i strafflagen och för att förhindra landsförräderibrott som är straffbara enligt 12 kap. i strafflagen.

De hemliga metoder för inhämtande av information som nämns ovan får användas för avslöjande av brott endast om det är fråga om landsförräderibrott eller terroristbrott.

Valet och användningen av hemliga metoder för inhämtande av information styrs av de polisrättsliga principer som nämns ovan och som har en viktig betydelse vid hemligt inhämtande av information.

Ett gemensamt drag hos användningsgrunderna för de hemliga metoderna för inhämtande av information är att de har definierats utgående från person och brott. De kan endast riktas mot

en sådan person eller användas för inhämtande av information endast om en sådan persons verksamhet som av grundad anledning kan antas i framtiden göra sig skyldig till eller redan ha gjort sig skyldig till ett brott som är förenat med ett visst hot om straff eller till förberedelse av ett sådant brott. Om det inte finns någon brottsavvärjande grund i anknytning till en viss person, är det inte möjligt att använda en hemlig metod för inhämtande av information i enlighet med polislagen. Inhämtande av annan underrättelseinformation måste således grunda sig på bevakning av öppna källor, polisens s.k. allmänna övervakning samt på information som skyddspolisen får av andra myndigheter och av privata aktörer via sitt samarbetsnätverk.

Enligt 10 § i polisförvaltningslagen ska skyddspolisen bekämpa inte bara brott som äventyrar rikets säkerhet utan också förehavanden som äventyrar rikets säkerhet. Begreppet förehavanden preciseras inte i polisförvaltningslagen eller i förarbetena till den. Det att skyddspolisens hemliga metoder för inhämtande av information ska grunda sig på brott medför att de inte kan användas för att inhämta information om sådana förehavanden som äventyrar statens säkerhet.

Den arbetsgrupp som utredde skyddspolisens administrativa ställning och resultatstyrning samt utvecklande av övervakningen behandlade frågan om huruvida skyddspolisens befogenheter att inhämta information kunde utsträckas till att också gälla avvärjande av förehavanden. Enligt arbetsgruppens slutrapport bör nya underrättelsebefogenheter övervägas för skyddspolisen för att den ska kunna bemöta förändringarna i sin omvärld. Det skulle handla om att av personer som agerar informationskällor och från datanät inhämta information som behövs för att bekämpa förehavanden som äventyrar rikets säkerhet, även om förehavandena inte har framskridit till det stadiet att de utgör brott som ska förhindras, avslöjas eller utredas.

Metoder för inhämtande av teleinformation

Teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, samtyckesbaserad teleövervakning och inhämtande av basstationsuppgifter är metoder för inhämtande av teleinformation.

Med teleavlyssning avses enligt 5 kap. 5 § 1 mom. i polislagen att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett sådant allmänt kommunikationsnät eller ett sådant därtill anslutet kommunikationsnät som avses i kommunikationsmarknadslagen (393/2003) avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 5 kap. 8 § i polislagen. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas göra sig skyldig till ett brott som avses i 5 kap. 5 § 2 mom. Eftersom personen ska nämnas i yrkandet om och tillståndet till teleavlyssning kan teleavlyssningen riktas endast mot den personen. I 2 mom. nämns de brott för vilkas förhindrande polisen får använda teleavlyssning. Brotten är 1) äventyrande av Finlands suveränitet, 2) krigsanstiftan, 3) landsförräderi, grovt landsförräderi, 4) spionerі, grovt spionerі, 5) röjande av statshemlighet, 6) olovlig underrättelseverksamhet, 7) brott som begåtts i terroristiskt syfte enligt 34 a kap. 1 § 1 mom. 2–7 punkten eller 2 mom. i strafflagen, 8) förberedelse till brott som begås i terroristiskt syfte, 9) ledande av terroristgrupp, 10) främjande av en terroristgrupps verksamhet, 11) meddelande av utbildning för ett terroristbrott, 12) deltagande i utbildning för ett terroristbrott, om gärningen är så allvarlig att den förutsätter fängelsestraff, 13) rekrytering för ett terroristbrott, 14) finansiering av terrorism, 15) finansiering av terroristgrupp, om gärningen är så allvarlig att den förutsätter fängelsestraff, eller 16) resa i syfte att begå ett terroristbrott, om gärningen är så allvarlig att den förutsätter fängelsestraff.

I 5 kap. 5 § 1 mom. i polislagen föreskrivs explicit att teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en viss person. Lagen möjliggör också av-

lyssning som gäller okända personers kommunikation, om en person med fog kan antas göra sig skyldig till ett brott som nämns ovan. För att förhindra brott kan polisen enligt 2 mom. ges tillstånd att rikta teleavlyssning mot en teleadress eller teleterminalutrustning som innehas eller sannolikt används av en person. Teleadressen eller teleterminalutrustningen behöver inte vara i personens ägo eller besittning, utan det räcker med att det finns ett samband mellan personen och den teleadress eller teleterminalutrustning som han eller hon använder eller sannolikt använder. Beviströskeln är inte hög till denna del. I praktiken ska ett nytt tillstånd till teleavlyssning sökas hos domstolen för varje ny teleadress eller teleterminalutrustning som en person använder eller sannolikt använder. Enligt 3 mom. kan polisen dessutom beviljas tillstånd till teleavlyssning, om det är nödvändigt för att avvärja en allvarlig fara som omedelbart hotar liv eller hälsa.

I 5 kap. 6 § i polislagen finns bestämmelser om inhämtande av information i stället för teleavlyssning. Bestämmelserna om teleavlyssning gällde ursprungligen telefonnät. När bestämmelserna om den nuvarande teleavlyssningen utfärdades avhjälptes vissa begränsningar som teknologibundenheten hade medfört. I 1 mom. sägs att om det är sannolikt att meddelanden som avses i 5 § och deras identifieringsuppgifter inte längre är tillgängliga genom teleavlyssning, kan polisen för att förhindra brott beviljas tillstånd att inhämta informationen hos ett teleföretag eller en sammanslutningsabonnent, under de förutsättningar som anges i 5 §. Det är fråga om beslag utifrån förutsättningarna för teleavlyssning, om åtgärden riktas mot ett teleföretag eller en sammanslutningsabonnent. Inhämtande av information i stället för teleavlyssning lämpar sig exempelvis för sådana fall där ett meddelande som åtkommits med stöd av en befogenhet till teleavlyssning har försvunnit eller förstörts men fortfarande tekniskt kan fås av ett teleföretag eller en sammanslutningsabonnent. Syftet med regleringen har varit att förhindra att förutsättningarna för användning av teleavlyssning kringgås genom att data beslagtas från ett teleföretag eller en sammanslutningsabonnent längs den väg data förmedlas.

I 5 kap. 6 § 2 mom. i polislagen sägs att om inhämtandet av information för utredning av innehållet i ett meddelande riktas mot en personlig teknisk anordning som lämpar sig för att sända och ta emot meddelanden och finns i direkt anslutning till en teleterminalutrustning eller mot förbindelsen mellan en sådan anordning och en teleterminalutrustning, kan polisen för att förhindra brott beviljas tillstånd till inhämtande av information i stället för teleavlyssning, om de förutsättningar som anges i 5 § finns. Utan bestämmelsen skulle information kunna inhämtas exempelvis som teknisk avlyssning, eftersom ett meddelande som passerat teleadressens gränssnitt och som vidareförmedlas till en personlig teknisk anordning av detta slag inte längre omfattas av befogenheten till teleavlyssning. Bluetooth-hörlurar är exempel på personliga anordningar som avses i momentet. Avlyssning av ett högtalarsamtal eller annat högljutt telefonsamtal är inte sådant inhämtande av information i stället för teleavlyssning som avses i momentet.

I 5 kap. 7 § 1 mom. i polislagen sägs att på yrkande av en polisman som avses i 2 kap. 9 § 1 mom. 1 punkten i tvångsmedelslagen (anhållningsberättigad polisman) beslutar domstolen om teleavlyssning och inhämtande av information i stället för teleavlyssning. Enligt 2 mom. kan tillstånd till teleavlyssning och till inhämtande av sådan information som avses i 6 § 2 mom. ges för högst en månad åt gången. Enligt 3 mom. ska följande nämnas i ett yrkande och i ett beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för teleavlyssningen eller för inhämtandet av information i stället för teleavlyssning grundar sig på, 4) giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning eller inhämtande av information enligt 6 § 2 mom., 5) den teleadress eller teleterminalutrustning som åtgärden riktas mot, 6) den anhållningsberättigade polisman som leder och övervakar utföran-

det av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning, 7) eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.

I yrkandet och beslutet ska detaljerade uppgifter läggas fram. I reformen av polislagen och tvångsmedelslagen (RP 224/2010 rd och RP 222/2010 rd) betonades skyldigheten att föra fram och motivera omständigheter som domstolen kan lägga till grund för sina egna slutsatser när det gäller förutsättningarna för användning av hemliga metoder för inhämtande av information. Förutsättningarna handlar om dels de allmänna förutsättningar som beskrivits ovan, dels de egentliga förutsättningarna enligt 5 kap. 5 och 6 § i polislagen.

Med teleövervakning avses enligt 5 kap. 8 § 1 mom. i polislagen att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät som avses i 5 § eller som har mottagits till en sådan adress eller utrustning samt att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att användningen av adressen eller utrustningen tillfälligt förhindras. Med identifieringsuppgifter avses i 2 § 8 punkten i lagen om dataskydd vid elektronisk kommunikation (516/2004) avsedda uppgifter om ett meddelande vilka kan förknippas med en abonnent eller användare och behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. I den gällande regleringen används en sådan definition av identifieringsuppgifter som härstammar från definitionen i 2 § 8 punkten i lagen om dataskydd vid elektronisk kommunikation. Det är omöjligt att definiera begreppet identifieringsuppgifter på ett uttömmande och entydigt sätt. Begränsningen av definitionen till uppgifter om ett meddelande innebär dock att sådan styrningstrafik mellan datorer som inte har samband med ett meddelande inte omfattas av skyddet för förtrolig kommunikation. För att förhindra brott kan polisen enligt 2 mom. ges tillstånd att rikta teleövervakning mot en teleadress eller teleterminalutrustning som innehas eller sannolikt används av en person som på grund av sina yttranden eller hotelser, sitt uppträdande eller i övrigt med fog kan antas göra sig skyldig till 1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år, 2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år, 3) utnyttjande av en person som är föremål för sexhandel, eller koppleri, 4) narkotikabrott, 5) förberedelse till brott som begås i terroristiskt syfte, eller 6) grovt tullredovisningsbrott.

I 5 kap. 9 § i polislagen finns bestämmelser om samtyckesbaserad teleövervakning. Med stöd av paragrafen gäller att med samtycke av den som innehar en teleterminalutrustning eller teleadress får polisen för att förhindra brott rikta teleövervakning mot teleadressen eller teleterminalutrustningen, om någon på grund av sina yttranden eller sitt uppträdande i övrigt med fog kan antas göra sig skyldig till 1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år, 2) ett brott som medför att teleadressen eller teleterminalutrustningen obehörigen innehas av någon annan, 3) brott mot besöksförbud, ofog som avses i 17 kap. 13 § 2 punkten i strafflagen eller hemfridsbrott som avses i 24 kap. 1 § 3 punkten i den lagen, om brottet begås genom användning av teleadressen eller teleterminalutrustningen, 4) något annat än ett i 3 punkten avsett brott som begås genom användning av teleadressen eller teleterminalutrustningen, eller 5) utnyttjande av person som är föremål för sexhandel. Att teleövervakningen gäller en teleadress eller teleterminalutrustning som innehas av den som ger samtycket avser faktisk besittning. Således kan exempelvis en arbetsgivare inte ge samtycke till teleövervakning av en mobiltelefon som är i en arbetstagares användning.

Enligt 5 kap. 10 § i polislagen ska domstolen på yrkande av en anhållningsberättigad tjänsteman besluta om teleövervakning för att förhindra eller avslöja brott samt om samtyckesbaserad teleövervakning som föreskrivs i 9 §. Tillstånd kan ges för högst en månad åt gången.

Tillstånd kan beviljas också för en bestämd tidsperiod som föregått beslutet. Tidsperioden kan vara längre än en månad.

Med inhämtande av basstationsuppgifter avses enligt 5 kap. 11 § 1 mom. i polislagen inhämtande av information om teleterminalutrustningar och teleadresser som redan är eller kommer att bli registrerade i ett telesystem via en viss basstation. Inhämtandet av basstationsuppgifter kan således gälla även teleadresser och teleterminalutrustningar som registreras i framtiden. Bestämmelsen i 2 mom. gäller förutsättningarna för inhämtande av basstationsuppgifter. Momentet innebär att polisen för att förhindra brott kan beviljas tillstånd att inhämta basstationsuppgifter när det är fråga om en basstation som vid en förmodad brottstidpunkt är belägen i närheten av en förmodad brottsplats och när det är fråga om en person som på grund av sina yttranden eller hotelser, sitt uppträdande eller annars med fog kan antas göra sig skyldig till ett brott som nämns i 8 § 2 mom., som gäller förutsättningarna för teleövervakning.

I 5 kap. 12 § i polislagen finns bestämmelser om förfarandet för beslut om inhämtande av basstationsuppgifter. Enligt 1 mom. ska beslut om inhämtande av basstationsuppgifter fattas av domstolen på yrkande av en anhållningsberättigad polisman. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman besluta om inhämtande av basstationsuppgifter till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas. Enligt 2 mom. beviljas tillstånd för en viss tidsperiod. Tillståndet kan gälla även information som hänför sig till tiden före beslutsfattandet, eftersom också information som hänför sig till tidpunkten före beslutet kan ha betydelse för förhindrande av ett brott. Det väsentliga är att informationens relevans kan motiveras.

Metoder av observationstyp

Metoder av observationstyp omfattar systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, teknisk spårning (teknisk spårning av en person), teknisk observation av utrustning och inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning samt sådan installation och avinstallation av anordningar, metoder eller programvara som stöder dessa metoder.

I 5 kap. 13 § i polislagen finns bestämmelser om systematisk observation. I 1 mom. ingår en allmän definition, enligt vilken med observation avses iakttagande av en viss person i hemlighet i syfte att inhämta information. Med systematisk observation avses enligt 2 mom. annan än kortvarig observation av en person som med fog kan antas göra sig skyldig till ett brott. På samma sätt som i enlighet med definitionen av begreppet observation används även systematisk observation i hemlighet, vilket också innebär att interaktion undviks. För att förhindra brott får polisen enligt 3 mom. systematiskt observera en person som avses i 2 mom., om det finns grundad anledning att misstänka att denne gör sig skyldig till ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år eller till stöld eller häleribrott. Enligt 4 mom. får observation enligt den aktuella paragrafen inte riktas mot utrymmen som används för stadigvarande boende. Observation genom sinnesiakttagelser i syfte att förhindra och avslöja brott får emellertid riktas också mot en person som befinner sig inom hemfridssfären.

I 5 kap. 14 § i polislagen finns bestämmelser om förfarandet för beslut om systematisk observation. Enligt 1 mom. ska beslut om systematisk observation fattas av en anhållningsberättigad polisman, och enligt 2 mom. får beslut fattas för högst sex månader åt gången. Bestämmelser om innehållet i beslut om systematisk observation finns i 3 mom.

Med förtäckt inhämtande av information avses enligt 5 kap. 15 § 1 mom. i polislagen inhämtande av information genom kortvarig interaktion med en viss person där falska, vilseledande

eller förtäckta uppgifter används för att hemlighålla polismannens uppdrag. Till skillnad från observation och systematisk observation kännetecknas utövandet av befogenheten uttryckligen av strävan att personligen träffa eller inleda någon motsvarande interaktion med den som det förtäckta inhämtandet av information riktas mot. Till skillnad från täckoperation handlar förtäckt inhämtande av information inte om infiltration, där strävan är att bygga upp ett långvarigt förtroendeförhållande. För att förhindra att informationsinhämtningen avslöjas får falska, vilseledande eller förtäckta uppgifter användas vid förtäckt inhämtande av information. För att förhindra brott får polisen enligt 2 mom. använda förtäckt inhämtande av information, om det på grund av en persons yttranden eller uppträdande i övrigt med fog finns anledning att anta att personen kommer att göra sig skyldig till 1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år, 2) utnyttjande av en person som är föremål för sexhandel, eller koppleri, 3) narkotikabrott, 4) förberedelse till brott som begås i terroristiskt syfte, 5) grovt tullredovisningsbrott, eller 6) stöld eller häleri som hänför sig till planmässig, organiserad, yrkesmässig, fortsatt eller upprepad brottslig verksamhet. Förtäckt inhämtande av information kan dock riktas även mot någon annan person än den som med fog kan antas komma att göra sig skyldig till brott.

Enligt 5 kap. 16 § 1 mom. i polislagen ska beslut om förtäckt inhämtande av information fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen, chefen för en polisinrättning eller en för uppdraget förordnad anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information. I 2 mom. finns bestämmelser om innehållet i beslut om förtäckt inhämtande av information. Beslutet ska fattas skriftligen. När det gäller utövning av befogenheten förutsätts det att det särskilt utses en polisman som ansvarar bl.a. för att åtgärden inte de facto är en täckoperation. I 3 mom. sägs att vid förändrade omständigheter ska beslutet vid behov ses över. Momentet ålägger den polisman som ansvarar för åtgärden att kontrollera att förutsättningarna för förtäckt inhämtande av information finns. Förtäckt inhämtande av information kan inte utföras i en bostad, inte ens i det fallet att polisen går in i bostaden med bostadsinnehavarens medverkan. Det anses emellertid inte ännu vara fråga om förtäckt inhämtande av information i en bostad då försändelsens mottagare ber den polisman som uppträder som bud vänta t.ex. i bostadens tambur medan mottagaren kvitterar försändelsen.

Med teknisk avlyssning avses enligt 5 kap. 17 § 1 mom. i polislagen att en viss persons samtal eller meddelande som inte är avsett för utomstående och i vilket avlyssnaren inte deltar avlyssnas, upptas eller behandlas på något annat sätt med hjälp av en teknisk anordning, metod eller programvara i syfte att ta reda på innehållet i samtalet eller meddelandet eller utreda deltagarna eller en i 4 mom. avsedd persons verksamhet. Sådan tangentbordsavlyssning som utförs med programvara eller en anordning i ett informationssystem omfattas också av definitionen av begreppet teknisk avlyssning enligt momentet. Skillnaden jämfört med sådan teknisk observation av utrustning som avses i 5 kap. 23 § är att teknisk observation av utrustning kan användas för att inhämta information om annan information som upptagits med eller behandlas på anordningen än information som innehåller kommunikation. Enligt 2 mom. får teknisk avlyssning inte riktas mot utrymmen som används för stadigvarande boende. Enligt 3 mom. har polisen rätt att för att förhindra brott utföra teknisk avlyssning utanför ett utrymme som används för stadigvarande boende i utrymmen eller platser där det kan antas att den person som inhämtandet av information gäller sannolikt befinner sig eller besöker. Med stöd av momentet kan teknisk avlyssning riktas mot en person som befinner sig i ett sådant hemfridsskyddat utrymme som avses i 24 kap. 11 § i strafflagen, förutsatt att utrymmet inte används för stadigvarande boende. Polisen kan också beviljas tillstånd att rikta teknisk avlyssning mot en person som befinner sig i en myndighetslokal och som berövats sin frihet på grund av brott. Enligt 4 mom. får teknisk avlyssning riktas mot en person som på grund av sina yttranden eller hotelser, sitt uppträdande eller i övrigt med fog kan antas göra sig skyldig till 1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år, 2) narkotikabrott, 3) förberedelse till brott som begås i terroristiskt syfte, eller 4) grovt tullredovisningsbrott. En

förutsättning för teknisk avlyssning är enligt 2 § 2 mom. dessutom att användningen av metoden kan antas vara av synnerlig vikt för förhindrande eller avslöjande av ett brott. Enligt 17 § 5 mom. har polisen trots 2 mom. i den paragrafen alltid rätt att utföra teknisk avlyssning, om det är nödvändigt för att en polisåtgärd tryggt ska kunna vidtas eller sådan överhängande fara avvärjas som hotar den persons liv eller hälsa som vidtar åtgärden eller den persons liv eller hälsa som ska gripas eller skyddas (stormningsavlyssning). Närmare bestämmelser om granskning och undersökning av upptagningar vid teknisk avlyssning och om avbrytande av teknisk avlyssning finns i 5 kap. 51, 52 och 56 § i polislagen. Även i dessa fall kan bestämmelserna om överskottsinformation i 5 kap. 53–55 § i polislagen bli tillämpliga. I fråga om teknisk avlyssning bör det nämnas att teleavlyssning och teleövervakning har planerats med tanke på telefonnät, medan informationsinhämtning som riktas mot krypterad kommunikation i datanät måste utföras delvis genom befogenheter av observationstyp, uttryckligen genom teknisk avlyssning.

Enligt 5 kap. 18 § 1 mom. i polislagen ska beslut om teknisk avlyssning som riktas mot en person som berövats sin frihet på grund av brott fattas av domstolen på yrkande av en anhållningsberättigad polisman. Beslut om annan än i 1 mom. avsedd teknisk avlyssning och alltid beslut om i 17 § 5 mom. avsedd stormningsavlyssning ska enligt 2 mom. fattas av en anhållningsberättigad polisman. Enligt 3 mom. kan tillstånd till teknisk avlyssning ges och beslut om teknisk avlyssning fattas för högst en månad åt gången. I 4 mom. finns bestämmelser om innehållet i ett yrkande och i ett beslut. Det har uppställts en särskild resultatförväntning för teknisk avlyssning. I yrkandet och beslutet bör därför nämnas fakta som tyder på att ett visst utrymme eller en annan plats är av en sådan beskaffenhet att den person som är föremål för inhämtandet av information sannolikt kan antas vistas där eller besöka utrymmet eller platsen. När teknisk avlyssning riktas mot ett utrymme behöver utrymmet dock inte specificeras lika exakt som den misstänkta personens bostad, om inte utrymmet är exakt känt när beslutet fattas.

Med optisk observation avses enligt 5 kap. 19 § 1 mom. i polislagen att man trots 24 kap. 6 § i strafflagen iakttar eller gör upptagningar av en viss person eller av ett utrymme eller någon annan plats med en kamera eller andra utplacerade tekniska anordningar, metoder eller programvaror. I likhet med teknisk avlyssning kan optisk observation riktas förutom mot ett utrymme eller en plats också mot en viss person. Optisk observation skiljer sig från observation och systematisk observation på så vis att man vid optisk observation använder utplacerade tekniska anordningar, metoder eller programvaror.

Enligt 2 mom. får optisk observation inte riktas mot ett utrymme som används för stadigvarande boende. Förbudet mot observation av bostäder gäller dock inte optisk observation i syfte att avvärja en fara, dvs. så kallad stormningsobservation. För att förhindra brott har polisen enligt 3 mom. rätt att rikta optisk observation mot personer utanför utrymmen som används för stadigvarande boende. Polisen kan ges tillstånd att rikta optisk observation också mot personer som befinner sig i en myndighetslokal och som berövats sin frihet på grund av brott. Optisk observation får riktas mot utrymmen eller platser som det på sannolika grunder kan antas att den person som inhämtandet av information gäller befinner sig i eller på eller besöker. En förutsättning för optisk observation av hemfridsskyddade utrymmen och andra platser som avses i 24 kap. 11 § i strafflagen och av personer som berövats sin frihet på grund av brott är enligt 4 mom. att personen i fråga på grund av sina yttranden eller hotelser, sitt uppträdande eller annars med fog kan antas göra sig skyldig till ett brott som avses i 17 § 4 mom., dvs. brott som ligger till grund för teknisk avlyssning. En förutsättning för annan optisk observation är att personen med fog kan antas göra sig skyldig till ett brott för vilket det föreskrivna strängaste straffet än fängelse i minst ett år. Enligt 5 mom. har polisen trots 2 mom. alltid rätt att utföra optisk observation, om det är nödvändigt för att en polisåtgärd tryggt ska kunna vidtas eller

sådan överhängande fara avvärjas som hotar den persons liv eller hälsa som vidtar åtgärden eller den persons liv eller hälsa som ska gripas eller skyddas.

Enligt 5 kap. 20 § 1 mom. i polislagen ska beslut om optisk observation fattas av domstolen på yrkande av en anhållningsberättigad polisman, om observationen riktas mot ett hemfridsskyddat utrymme eller en annan plats som avses i 24 kap. 11 § i strafflagen eller mot en person som berövats sin frihet på grund av brott. Enligt 2 mom. ska beslut om stormningsobservation som avses i 19 § 5 mom. och om annan än i 1 mom. avsedd optisk observation fattas av en anhållningsberättigad polisman. Enligt 3 mom. kan tillstånd till optisk observation ges och beslut om optisk observation fattas för högst en månad åt gången. I 4 mom. finns bestämmelser om innehållet i ett yrkande och i ett beslut om optisk observation.

Teknisk spårning definieras i 5 kap. 21 § 1 mom. i polislagen, och enligt momentet avses med teknisk spårning att förflyttning av föremål, ämnen eller egendom spåras med hjälp av radiosändare som fästs eller som redan finns på objektet eller med hjälp av någon annan liknande teknisk anordning, metod eller programvara. Enligt 2 mom. får polisen för att förhindra brott rikta teknisk spårning mot föremål, ämnen eller egendom som är föremål för ett brott eller som en person antas inneha eller använda, om det på grund av dennes yttranden eller hotelser, uppträdande eller annars med fog kan antas att personen i fråga kommer att göra sig skyldig till ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst ett år. I 3 mom. föreskrivs det om teknisk spårning av en person. Om syftet med teknisk spårning är att följa hur en person förflyttar sig genom att en spårningsanordning fästs i de kläder som han eller hon bär eller i ett föremål som han eller hon bär med sig (teknisk spårning av en person), får åtgärden genomföras bara om personen i fråga med fog kan antas begå ett brott som avses i 17 § 4 mom., dvs. när även teknisk avlyssning är möjlig. Enligt 4 mom. har polisen dessutom rätt att utföra teknisk spårning om det är nödvändigt för att en polisåtgärd tryggt ska kunna vidtas eller sådan överhängande fara avvärjas som hotar den persons liv eller hälsa som vidtar åtgärden eller en persons liv eller hälsa som ska gripas eller skyddas (stormningsspårning).

Enligt 5 kap. 22 § 1 mom. i polislagen ska beslut om teknisk spårning av en person fattas av domstolen på yrkande av en anhållningsberättigad polisman. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman besluta om sådan spårning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas. Enligt 2 mom. ska en anhållningsberättigad polisman besluta om spårning som avses i 21 § 4 mom. och om annan än i 1 mom. avsedd teknisk spårning. Enligt 3 mom. kan tillstånd ges och beslut fattas för högst sex månader åt gången. I 4 mom. anges vad som ska nämnas i ett yrkande och i ett beslut om teknisk spårning.

I 5 kap. 23 § 1 mom. i polislagen definieras teknisk observation av utrustning. Med teknisk observation av utrustning avses att en funktion, informationsinnehållet eller identifieringsuppgifterna i en dator eller i en liknande teknisk anordning eller i dess programvara på något annat sätt än enbart genom sinnesförnimmelser observeras, upptas eller behandlas på något annat sätt för att utreda omständigheter som är av betydelse för förebyggande av ett brott. Teknisk observation av utrustning kan riktas mot tekniska anordningar och över huvud taget mot information som en misstänkt person lagrat i en anordning. Sådan information kan ingå i dokument som lagrats i en anordning. Teknisk observation av utrustning kan användas för att följa interaktionen mellan en person och en teknisk anordning. Det är meningen att 2 mom. ska dra upp en gräns i förhållande till teletvångsmedel. Genom teknisk observation av utrustning får enligt momentet inte inhämtas information om innehållet i ett meddelande eller om identifieringsuppgifter som avses i 8 §. Polisen får rikta teknisk observation av utrustning mot en dator eller en annan liknande teknisk anordning som personen i fråga sannolikt använder, eller mot en funktion i dess programvara. Av lagen och motiveringen till den framgår åtminstone indi-

rekt att med innehållet i ett meddelande avses uttryckligen innehållit i ett meddelande visavi teleavlyssning och teknisk avlyssning exempelvis när kommunikationen sker i realtid mellan två människor via exempelvis dator eller smarttelefon. Dokument som redan upptagits eller lagrats på anordningen och som inte i realtid står i kontakt med den tekniska avlyssningen eller teleavlyssningen omfattas således av teknisk observation av utrustning. Teknisk observation av utrustning kan användas för s.k. tangentbordsavlyssning bara till den del den som använder anordningen inte skriver ett meddelande. För tangentbordsavlyssning som gäller kommunikation ska polisen utöva befogenheten för teknisk avlyssning enligt 17 § för vilken de brott som berättigar åtgärden är desamma som för observation av utrustning. Enligt 3 mom. kan polisen för förhindrande av brott ges tillstånd till att utföra teknisk observation av utrustning, om det på grund av en persons yttranden, hotelser, uppträdande eller annars med fog kan antas att denne kommer att göra sig skyldig till ett brott som avses i 17 § 4 mom.

Enligt 5 kap. 24 § 1 mom. i polislagen ska beslut om teknisk observation av utrustning fattas av domstolen på yrkande av en anhållningsberättigad polisman. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman besluta om teknisk observation av utrustning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas. Enligt 2 mom. kan tillstånd meddelas för högst en månad åt gången. I 3 mom. anges vad som ska nämnas i ett yrkande och i ett beslut om teknisk observation av utrustning.

För att förhindra brott får polisen enligt 5 kap. 25 § 1 mom. i polislagen med en teknisk anordning inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning, när det är fråga om brott för vilket det föreskrivna strängaste straffet är fängelse i minst ett år. För inhämtande av de uppgifter som avses i 1 mom. får polisen enligt 2 mom. bara använda sådana tekniska anordningar som endast kan användas för identifiering av teleadresser och teleterminalutrustningar. Kommunikationsverket ska kontrollera att de tekniska anordningarna uppfyller kraven enligt det momentet och att de inte på grund av sina egenskaper orsakar skadliga störningar i ett allmänt kommunikationsnäts anordningar eller tjänster. Beslut om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning fattas enligt 3 mom. av en anhållningsberättigad polisman.

Enligt 5 kap. 26 § 1 mom. i polislagen har en polisman rätt att fästa en anordning, metod eller programvara som används för teknisk observation på föremål, ämnen, egendom, i utrymmen och andra platser eller informationssystem som åtgärden riktas mot, om det behövs för observationen. För att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran har polismannen då rätt att i hemlighet ta sig in i ett ovan nämnt utrymme eller på en ovan nämnd plats eller i ett ovan nämnt informationssystem samt att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemens säkerhetssystem. Det föreskrivs särskilt om husrannsakan. Enligt 2 mom. får anordningar, metoder och programvara som används för teknisk observation installeras i utrymmen som används för stadigvarande boende endast om domstolen har gett tillstånd till det på yrkande av en anhållningsberättigad polisman eller om installationen är nödvändig i sådana fall som avses i 17 § 5 mom., 19 § 5 mom. eller 21 § 4 mom. En anordning, metod eller programvara får utan domstolstillstånd installeras i ett utrymme som används för stadigvarande boende för att avvärja en fara i sådana fall som avses i momentet, dvs. i situationer där det är fråga om s.k. stormningsobservation.

Täckoperationer och bevisprovokation genom köp

Bestämmelserna om förutsättningarna för täckoperationer och bevisprovokation genom köp är speciellt strikta på grund av att metoderna har en karaktär som inte är typisk för hemligt inhämtande av information.

Med täckoperation avses enligt 5 kap. 28 § 1 mom. i polislagen planmässigt inhämtande av information om en viss person eller dennes verksamhet genom infiltration, där falska, vilseledande eller förtäckta uppgifter eller registeranteckningar används eller falska handlingar framställs eller används för att förvärva förtroende som behövs för inhämtandet av information eller för att förhindra att inhämtandet av information avslöjas. Enligt 2 mom. får polisen rikta en täckoperation mot en person som är misstänkt för brott, om han eller hon med fog kan misstänkas för något annat i 10 kap. 3 § i tvångsmedelslagen avsett brott än grovt ordnande av olaglig inresa eller grovt tullredovisningsbrott eller ett brott som avses i 17 kap. 18 § 1 mom. 1 punkten i strafflagen. En förutsättning är dessutom att inhämtandet av information måste anses vara behövligt på grund av att den brottsliga verksamheten är planmässig, organiserad eller yrkesmässig eller på grund av att det kan antas att den fortsätter eller upprepas. I 3 mom. föreskrivs det om datanätsbaserade täckoperationer. Enligt momentet får polisen rikta en datanätsbaserad täckoperation mot en person som är misstänkt för brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år eller om det är fråga om ett brott som avses i 17 kap. 19 § i strafflagen.

Bestämmelserna om husrannsakan får inte kringgås genom täckoperationer. Därför är täckoperationer tillåtna i en bostad bara om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden. Det föreskrivs särskilt om husrannsakan.

I 5 kap. 29 § i polislagen finns bestämmelser om brottsförbud och i 30 § finns bestämmelser om deltagande i en organiserad kriminell sammanslutnings verksamhet och i kontrollerade leveranser. I 31 och 32 § föreskrivs det om framställning om och plan för en täckoperation och om beslut om en täckoperation. I 34 och 33 § föreskrivs det om utvidgad täckoperation och om beslut om förutsättningarna för täckoperation.

Innan ett beslut om en täckoperation kan fattas måste det finnas en framställning om och en plan för täckoperationen. Enligt 5 kap. 31 § 1 mom. i polislagen ska följande nämnas i en framställning om täckoperation: 1) den som föreslagit åtgärden, 2) den person, tillräckligt specificerad, som är föremål för inhämtandet av information, 3) det brott, tillräckligt specificerat, som ligger till grund för åtgärden, 4) syftet med täckoperationen, 5) behovet av täckoperationen, 6) övriga uppgifter som behövs för att bedöma förutsättningarna för täckoperationen. Över genomförandet av en täckoperation ska enligt 2 mom. en sådan skriftlig plan göras upp som innehåller väsentlig och tillräckligt detaljerad information för beslutsfattandet om och genomförandet av täckoperationen. Vid förändrade omständigheter ska planen vid behov ses över.

I 5 kap. 32 § i polislagen finns bestämmelser om beslut om en täckoperation. Beslut om en täckoperation ska fattas av chefen för centralkriminalpolisen eller chefen för skyddspolisen. Chefen för centralkriminalpolisen, chefen för skyddspolisen, chefen för polisinrättningen eller en för uppdraget förordnad anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information ska besluta om täckoperationer som genomförs uteslutande i datanät (1 mom.). Beslut om en täckoperation kan meddelas för högst sex månader åt gången (2 mom.). Enligt 3 mom. ska beslut om en täckoperation fattas skriftligen. I beslutet ska följande nämnas: 1) den som föreslagit åtgärden, 2) den polisenhet som genomför täckoperationen och den polisman som ansvarar för genomförandet av täckoperationen, 3) identifikationsuppgifterna för de polismän som genomför täckoperationen, 4) det brott som ligger till grund för inhämtandet av information, 5) den som är föremål för täckoperationen och som med fog kan antas begå det brott som avses i 4 punkten, 6) de fakta som brottsmisstanken och förutsättningarna för täckoperationen grundar sig på, 7) täckoperationens syfte och genomförandeplan, 8) beslutets giltighetstid, 9) huruvida åtgärder enligt 30 § får utföras inom ramen för täckoperationen, de fakta som åtgärderna grundar sig på samt eventuella begränsningar och villkor för täckoperationen. Vid förändrade förhållanden ska beslutet vid behov ses över. Beslut om avslutande av en täckoperation ska fattas skriftligen (4 mom.).

I 5 kap. 33 § i polislagen föreskrivs det om domstolens avgörande om huruvida det finns förutsättningar för en täckoperation. Om avsikten är att information som fåtts genom en täckoperation ska användas i rättegång såsom en utredning till stöd för att någon är skyldig, ska enligt paragrafen den polisman som fattat beslut om täckoperationen låta domstolen avgöra om det fanns sådana förutsättningar för en täckoperation som avses i 28 § 2 mom. eller om det var fråga om en täckoperation i sådana fall som avses i 3 §.

Med bevisprovokation genom köp avses enligt 5 kap. 35 § 1 mom. i polislagen ett köpeanbud eller ett köp av ett föremål, ett ämne, egendom eller en tjänst som polisen för att förhindra ett brott gör i syfte att ta om hans eller påträffa ett föremål, ett ämne eller egendom som har samband med det brott som ska förhindras. En förutsättning för köp av annat än ett provparti är att köpet är nödvändigt för genomförandet av bevisprovokation genom köp. Enligt 2 mom. får polisen i syfte att förhindra brott genomföra bevisprovokation genom köp, om det är fråga om ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år eller stöld eller häleribrott och det är sannolikt att något av de mål som nämns i 1 mom. kan uppnås genom bevisprovokationen. Enligt 3 mom. får den som genomför bevisprovokation genom köp utföra bara sådant inhämtande av information som är nödvändigt för att genomföra bevisprovokationen. Bevisprovokationen genom köp ska genomföras så att den inte får den person som är föremål för åtgärden eller någon annan att begå ett brott som han eller hon inte annars skulle begå. Bestämmelserna om husrannsakan får inte heller kringgås genom bevisprovokation genom köp. Enligt 4 mom. gäller därför att bevisprovokation genom köp är tillåten i en bostad bara om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden. Det föreskrivs särskilt om husrannsakan.

Bestämmelser om beslut om bevisprovokation genom köp, plan för genomförande av bevisprovokation genom köp och beslut om genomförande av bevisprovokation genom köp finns i 5 kap. 35–38 § i polislagen.

I 5 kap. 39 § i polislagen finns bestämmelser om säkerheten för en polisman vid förtäckt inhämtande av information, vid en täckoperation och vid bevisprovokation genom köp. En anhållningsberättigad polisman får besluta att en polisman som ska genomföra förtäckt inhämtande av information, en täckoperation eller bevisprovokation genom köp ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att polismannens säkerhet ska kunna tryggas (1 mom.). Avlyssningen och observationen får upptas. Upptagningarna ska utplånas så snart de inte behövs för att trygga polismannens säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har samband med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller lämnats därhän (2 mom.).

Styrd användning av informationskällor samt kontrollerade leveranser

I 5 kap. 40–43 § i polislagen finns bestämmelser om användning av informationskällor samt kontrollerade leveranser. Med användning av informationskällor avses enligt 40 § 1 mom. annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av i 1 kap. 1 § avsedda uppgifter av personer som inte hör till polisen eller till någon annan förundersökningsmyndighet (informationskälla). Enligt 2 mom. får polisen be att en för ändamålet godkänd informationskälla som har lämpliga personliga egenskaper och är registrerad och har samtyckt till inhämtandet av information inhämtar den information som avses i 1 mom. (styrd användning av informationskällor). I 3 mom. sägs att vid styrd användning av informationskällor får en informationskälla inte ombes att inhämta information på ett sådant sätt som förutsätter utövande av myndighetsbefogenheter eller som äventyrar informationskällans eller någon annans liv eller hälsa. Innan styrd användning av informationskällor inleds ska informat-

ionskällan upplysas om sina rättigheter och skyldigheter och i synnerhet om vad som är tillåten och förbjuden verksamhet enligt lag. Informationskällans säkerhet ska vid behov tryggas under och efter inhämtandet av information.

I 5 kap. 41 § i polislagen finns bestämmelser om behandling av uppgifter om en informationskälla och betalning av arvode. Enligt 1 mom. får uppgifter om en informationskälla registreras i ett personregister. På behandlingen av uppgifterna tillämpas lagen om behandling av personuppgifter i polisens verksamhet (761/2003). Till en registrerad informationskälla kan enligt 2 mom. betalas arvode. Av grundad anledning kan arvode betalas även till en oregistrerad informationskälla. Särskilda bestämmelser gäller om skatteplikt för arvodet.

I 5 kap. 42 § i polislagen finns bestämmelser om beslut om styrd användning av informationskällor. Enligt 1 mom. ska beslut om styrd användning av informationskällor fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen, chefen för en polisinrättning eller av en för uppdraget förordnad anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information. Enligt 2 mom. kan beslut om styrd användning av informationskällor meddelas för högst sex månader åt gången. I 3 mom. anges vad som ska nämnas i beslutet samt att beslutet ska fattas skriftligen. I beslutet ska följande nämnas: 1) den som föreslagit åtgärden, 2) den polisenhet som genomför inhämtandet av information och den polisman som ansvarar för genomförandet av detta, 3) identifikationsuppgifterna för informationskällan, 4) grunden för åtgärden, 5) syftet med inhämtandet av information och planen för genomförandet av detta, 6) beslutets giltighetstid, 7) eventuella begränsningar och villkor för den styrda användningen. När omständigheterna förändras ska beslutet vid behov ses över. Beslut om att styrd användning ska avslutas ska fattas skriftligen (4 mom.).

I 5 kap. 43 § i polislagen finns bestämmelser om kontrollerade leveranser och förutsättningar för sådana. Enligt 1 mom. får polisen avstå från att ingripa i transporten eller någon annan leverans av föremål, ämnen eller egendom eller dröja med att ingripa, om det behövs för identifiering av personer som medverkar i ett brott som håller på att begås eller för att förhindra ett brott som är allvarligare eller en brottslig verksamhet som är mera omfattande än det brott som håller på att begås (kontrollerad leverans). Enligt 2 mom. får polisen använda kontrollerade leveranser för att förhindra brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år. Det förutsätts dessutom att de kontrollerade leveranserna kan övervakas och att det går att ingripa i dem vid behov. Åtgärden får inte heller orsaka betydande fara för någons liv, hälsa eller frihet eller avsevärd risk för betydande miljö-, egendoms- eller förmögenhetsskada. Det föreskrivs särskilt om myndighetssamarbete för att genomföra kontrollerade leveranser. I fråga om internationella kontrollerade leveranser som hör samman med internationella avtal eller andra förpliktelser som är bindande för Finland gäller enligt 3 mom. dessutom vad som särskilt föreskrivs i lag. I 5 kap. 44 § finns bestämmelser om beslut om kontrollerade leveranser.

Förundersökningsbefogenheter och tvångsmedel

Skyddspolisen är en förundersökningsmyndighet som avses i förundersökningslagen (805/2011). I 2 kap. 1 § i förundersökningslagen finns bestämmelser om myndigheterna vid förundersökning. Enligt 1 mom. görs förundersökning av polisen. Förundersökningsmyndigheter är enligt 2 mom. förutom polisen även gränsbevaknings-, tull- och militärmyndigheterna, enligt vad som föreskrivs om deras förundersökningsbefogenheter i gränsbevakningslagen (578/2005), lagen om brottsbekämpning inom Tullen (623/2015) och lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014).

I 2 kap. 9 § 1 mom. 1 punkten i tvångsmedelslagen (806/2011) nämns några anhållningsberättigade polistjänstemän. Enligt 1 mom. beslutar en anhållningsberättigad tjänsteman om anhål-

lande. Anhållningsberättigade tjänstemän är 1) polisöverdirektören, vid Polisstyrelsen polisdirektör, polisöverinspektör och polisinspektör, polischef, biträdande polischef, vid centralkriminalpolisen chefen för centralkriminalpolisen och biträdande chef, vid skyddspolisen chefen för skyddspolisen, biträdande chef som förordnats att sköta förundersökningsuppgifter, avdelningschef som förordnats att sköta förundersökningsuppgifter, överinspektör och inspektör som förordnats att sköta förundersökningsuppgifter, kriminalöverinspektör, kriminalinspektör, kriminalöverkommissarie, överkommissarie, kriminalkommissarie och kommissarie.

Skyddspolisen kan således i enlighet med sitt uppdrag exempelvis för att utreda ett brott använda hemliga tvångsmedel enligt 10 kap. i tvångsmedelslagen och utöva befogenheterna för beslag samt kopiering av handlingar enligt 7 kap. i tvångsmedelslagen. Eftersom skyddspolisen bara sällan utför förundersökning, blir tvångsmedelslagen bara relativt sällan tillämplig inom skyddspolisens verksamhet.

I slutrapporten av den arbetsgrupp som utredde skyddspolisens administrativa ställning och resultatstyrning samt utvecklande av övervakningen nämndes att om skyddspolisens befogenheter för underrättelseinhämtning utvidgas, bör man i syfte att säkerställa en rättvis rättegång överväga en begränsning av skyddspolisens förundersökningsuppgifter och förundersökningsbefogenheter. Skyddspolisen ska fortsättningsvis enligt behov kunna delta i förundersökningar i egenskap av expertmyndighet.

Samarbete mellan skyddspolisen och andra myndigheter som har betydelse för den nationella säkerheten

De myndigheter som nämns ovan bedriver ett nära samarbete med varandra på det sätt som varje myndighets uppgift kräver med avseende på myndighetens ansvarsområde.

Mellan skyddspolisens och polisinrättningarnas verksamhet finns centrala beröringspunkter som gäller upprätthållande av säkerheten. Skyddspolisen och polisinrättningarna utbyter information om den allmänna ordningen och säkerheten samt brottsbekämpningen och samarbetar även i övrigt. Skyddspolisen har ett nära samarbete med centralkriminalpolisen i synnerhet när det gäller att bekämpa terrorism och är sakkunnig i terroristbrottsutredningar. Dessutom samarbetar skyddspolisen med centralkriminalpolisen när det gäller hemligt inhämtande av information.

För att skydda den nationella säkerheten samarbetar skyddspolisen med den militära underrättelseinhämtningen. Samarbetet med den militära underrättelseinhämtningen behandlas närmare i andra delar av betänkandet.

Samarbetet med Migrationsverket hänför sig framför allt till att utreda förutsättningarna för inresa. För detta ger skyddspolisen utlåtanden till stöd för Migrationsverkets beslutsfattande. Skyddspolisen ger också utlåtanden i medborgarskapsärenden och i andra ärenden där uppgifter behöver lämnas till stöd för Migrationsverkets beslutsfattande. Vidare samarbetar skyddspolisen med Migrationsverkets informationstjänst när det gäller utbyte av information och även i övrigt. Landinformationen vid Migrationsverket producerar landinformation på strategisk nivå om utreseländer för asylsökande, kvotflyktingar och invandrare. Informationen gäller bl.a. utreseländernas politiska och sociala förhållanden, människorätts- och säkerhetssituation, lagstiftning och omständigheter i det dagliga livet. Migrationsverkets informationsproduktion gäller delvis samma länder som skyddspolisens, och därför utbyter dessa myndigheter strategisk information om omvärlden och bedriver exempelvis ömsesidigt utbildningssamarbete.

Skyddspolisens och gränsbevakningsväsendets samarbete hänför sig närmast till uppgifter inom gränsbevakning, in- och utresekontroller samt brottsbekämpning. De huvudsakliga samarbetsformerna utgörs av informationsutbyte och handräckning mellan myndigheterna.

Dessutom föreskrivs det särskilt om samarbetet mellan polis-, tull- och gränsbevakningsväsendet. För att skydda den nationella säkerheten bedriver skyddspolisen nära samarbete med alla PTG-myndigheter. Skyddspolisen är inte någon egentlig PTG-myndighet, men deltar i PTG-myndigheternas samarbete i ärenden som berör skyddspolisens verksamhetsområde.

Skyddspolisen är kund hos den lägesbildsverksamhet som Cybersäkerhetscentret vid Kommunikationsverket ansvarar för, och enligt behov producerar skyddspolisen information för lägesbilden. Skyddspolisen samarbetar med Cybersäkerhetscentrets lägescentral när det gäller att förutse hot mot informationssäkerheten som riktas mot den nationella säkerheten och att utreda sådana kränkningar av informationssäkerheten.

Bekämpning av hot mot informationssäkerheten

Den elektroniska kommunikationens samt datanätens och informationssystemens funktion och frihet från störningar skyddas med hjälp av informationssäkerhet. Med informationssäkerhet avses administrativa och tekniska åtgärder genom vilka det säkerställs att information är tillgänglig endast för dem som har rätt att använda den (konfidentialitet), att informationen inte kan ändras av andra än dem som har rätt till detta (integritet) samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen (tillgänglighet).

De aktörer som använder elektroniska kommunikationsnät och kommunikationstjänster sörjer för sin informationssäkerhet med olika metoder. Informationssäkerheten kan upprätthållas med exempelvis informationsförvaltningsmetoder och genom att uppställa tekniska begränsningar för användningen av ett kommunikationsnät eller en tjänst. Statsförvaltningens enhetliga karaktär innebär att förvaltningens informationssäkerhet kan styras centraliserat och med stöd av enhetliga principer. Finansministeriet styr och leder det allmänna utvecklandet av informationssäkerheten inom den offentliga förvaltningen och informationssäkerheten inom statsförvaltningen samt IKT-beredskapen. Finansministeriets styrande uppgift grundar sig på bl.a. lagen om styrning av informationsförvaltningen inom den offentliga förvaltningen (634/2011) och lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013).

Syftet med lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) är att under normala förhållanden och vid störningar under normala förhållanden samt under undantagsförhållanden säkerställa att den kommunikation som samarbetet mellan den högsta statsledningen och de myndigheter och andra aktörer som är viktiga med tanke på säkerheten i samhället förutsätter är störningsfri och obruten samt att säkerställa att den information som behövs vid beslutsfattandet och ledningen är lättillgänglig, integrerad och konfidentiell. I lagen finns bestämmelser om ett säkerhetsnät (TUVE), som förenar statsledningen, ministerierna, försvarsmakten, gränsbevakningsväsendet, polisen och räddningsväsendet i samma datakommunikationsnät.

Centraliserad styrning av informationssäkerheten är inte möjlig inom den privata sektorn, utan nivån på informationssäkerheten och de lösningar som valts för att upprätthålla informationssäkerheten varierar enligt varje organisations egna behov och prioriteringar. Såväl inom förvaltningen som inom den privata sektorn grundar sig upptäckten av och skyddandet mot hot mot informationssäkerheten i praktiken på kommersiella informationssäkerhetsprogram och informationssäkerhetstjänster. En del av statsförvaltningen och av de företag som är kritiska

med tanke på försörjningsberedskapen använder i sitt skyddande också Kommunikationsverkets system för att upptäcka och varna för allvarliga kränkningar av informationssäkerheten (HAVARO), som behandlas längre fram.

Bestämmelserna i 272 § i lagen om tjänster inom elektronisk kommunikation (917/2014) ger sådana företag, sammanslutningar och myndigheter som använder sig av elektroniska kommunikationstjänster rätt att för att sörja för sin informationssäkerhet analysera innehållet i meddelanden till och från sitt nät bl.a. i syfte att upptäcka, förhindra och utreda störningar som kan inverka menligt på informationssäkerheten och göra störningarna föremål för förundersökning.

Automatisk analys av innehållet i kommunikationen gäller innehållet i alla de meddelanden som kommer in till och som skickas ut från datanät eller informationssystem hos den som använder sig av automatisk analys. Det huvudsakliga syftet med analysen är att upptäcka sabotageprogrammens försök att tränga in i informationssystemet samt den kommunikation som sabotageprogram som eventuellt redan trängt in i systemet för med sina värdar.

De skadliga programmen och kommandona identifieras i en första fas vid automatisk analys av innehållet utgående från på förhand fastställda attribut, och innehållet i meddelandet kommer då inte till den fysiska personens kännedom. Om det är uppenbart att ett meddelande som kommit fram vid automatisk filtrering innehåller ett sabotageprogram och informationssäkerheten inte kan säkerställas med automatiska medel, tillåter 272 § i lagen om tjänster inom elektronisk kommunikation att företaget, sammanslutningen eller myndigheten tar innehållet i meddelandet till manuell behandling.

Cybersäkerhetscentret vid Kommunikationsverket är en nationell informationssäkerhetsmyndighet vars uppgifter omfattar att förebygga, samla information om och utreda sådana kränkningar av informationssäkerheten som anknyter till de allmänna kommunikationsnäten och via dem är riktade mot finländska aktörer samt att informera om betydande hot mot informationssäkerheten. Enligt cybersäkerhetsstrategin har Cybersäkerhetscentret också till uppgift att producera och upprätthålla en sammanställd lägesbild över cybersäkerheten. Cybersäkerhetscentret samlar in uppgifter om händelser i datanäten och förmedlar dem till olika aktörer samt utformar och delar cybersäkerhetens sammanställda lägesbild. Cybersäkerhetscentrets kunder kan utnyttja lägesbildsuppgifterna när de organiserar och prioriterar sin beredskap.

Vid formandet av lägesbilden utnyttjas utöver nationella källor också Cybersäkerhetscentrets internationella samarbetsnätverk, som bygger på frivillighet och ömsesidigt förtroende. Moderorganisationerna för de GovCERT-grupper som ingår i samarbetsnätverket är placerade i olika segment inom statsförvaltningen i sina respektive länder. Exempelvis Sveriges CERT-SE är en del av ett civilt beredskapsverk medan Tysklands CERT-BUND finns inom inrikesministeriets förvaltningsområde. I en del stater har CERT-grupperna placerats inom försvarsministeriets förvaltningsområde och i en del är CERT-grupperna verksamma som en del av underrättelsemyndigheten, exempelvis i Förenade kungariket (Government Communications Headquarters, GCHQ).

HAVARO är ett system för att upptäcka och varna för kränkningar av informationssäkerheten vilket Cybersäkerhetscentret vid Kommunikationsverket erbjuder företag som är kritiska med tanke på försörjningsberedskapen och aktörer inom statsförvaltningen. Verksamheten grundar sig på 272 § i lagen om tjänster inom elektronisk kommunikation. Ett syfte med HAVARO är att med olika identifierare identifiera skadlig nättrafik och avancerade nätattacker som äventyrar informationssäkerheten (Advanced Persistent Threat, APT). Ett annat syfte med systemet är att stödja möjligheterna att utforma en bättre lägesbild över de hot mot informationssäkerheten som riktas mot finländska datanät. De tekniska identifierare av sabotageprogram som

utnyttjas i systemet grundar sig huvudsakligen på information som Cybersäkerhetscentret fått av inhemska och utländska samarbetspartner.

Skyddspolisens informationsinhämtning utomlands

Enligt 10 § i polisförvaltningslagen har skyddspolisen till uppgift att avvärja hot av utländskt ursprung som riktas mot statens säkerhet. Internationell terrorism, spionage som främmande stater riktar mot Finland och landets intressen samt planering, tillverkning, spridning och användning av massförstörelsevapen är exempel på hot av utländskt ursprung. Enligt skyddspolisens gällande uppgiftsförordnande har ämbetsverket också till uppgift att analysera statens säkerhetspolitiska omgivning och upprätthålla en internationell lägesbild inom sitt verksamhetsområde. Skyddspolisen rapporterar till andra säkerhetsmyndigheter och till Finlands högsta statsledning om hur den internationella säkerhetspolitiska omgivningen utvecklar sig.

Den parlamentariska poliskommitténs betänkande (kommittébetänkande 1986:16) som låg till grund för stiftandet av polisförvaltningslagen betonar att av statens självständighet följer som ett värde att staten måste ha beredskap att hela tiden skydda sin yttre säkerhet. Enligt betänkandet kan den yttre säkerheten äventyras av alla sådana strävanden som har en skadlig inverkan på rikets rättigheter och intressen eller på relationerna mellan Finland och främmande stater. Enligt den parlamentariska poliskommittén är det uttryckligen skyddspolisen som har en central roll vid avvärjandet av sådana faror och olägenheter.

Finlands säkerhetspolitiska omgivning har internationaliserats kraftigt efter det att den parlamentariska poliskommitténs betänkande publicerades. Information om andra länder har en allt större betydelse när det gäller att skydda de säkerhetsintressen som skyddspolisen ansvarar för.

Det finns inga bestämmelser om skyddspolisens inhämtande av information utomlands. Skyddspolisens inhämtande av information grundar sig på utövning av de befogenheter som enligt polislagen gäller i fråga om förhindrande och avslöjande av brott. Dessa befogenheter kan utövas endast på finländskt territorium.

Skyddspolisens möjligheter att få information om utländska förhållanden stöder sig i praktiken på det internationella underrättelsesamarbete som skyddspolisen bedriver, på bevakningen av öppna källor samt på skyddspolisens verksamhet med egna kontaktpersoner.

Skyddspolisen och dess föregångare har sedan Finland blev självständigt bedrivit ett omfattande bilateralt och multilateralt samarbete med utländska underrättelse- och säkerhetstjänster. Med hjälp av samarbetet säkerställs det att den underrättelseinformation om utländska förhållanden som behövs för att upprätthålla statens säkerhet kan fås. Till följd av säkerhetsfrågornas allmänna globaliseringsutveckling och den ökade betydelse av underrättelseinformation om utländska förhållanden som blivit följden av detta har skyddspolisen under de senaste åren planenligt breddat sitt internationella samarbetsnätverk så att det för närvarande anses omfatta underrättelse- och säkerhetsmyndigheterna i alla länder som är viktiga med tanke på Finlands säkerhet.

De internationella samarbetsförfaranden som betjänar brottsbekämpningen måste hållas isär från det internationella underrättelsesamarbetet. Inom skyddspolisens verksamhetsområde är betydelsen av dessa samarbetsförfaranden liten. Ett viktigt skäl till detta är att de personer som skyddspolisens brottsbekämpning riktas mot i allmänhet agerar för en främmande stats räkning och ofta även som denna stats tjänstemän agerar mot Finlands intressen. En stat som drar nytta av en brottslig gärning ger i praktiken inte den stat som brottet riktas mot – exempelvis Finland – någon sådan hjälp som behövs för att förhindra, avslöja eller utreda brottet.

Skyddspolisens bevakning av öppna källor gällande främmande länder täcker hela ämbetsverkets verksamhetsområde. Den information som inhämtas från öppna källor sammanställs med information från andra källor för att åstadkomma en analyserad säkerhetslägesbild över Finlands internationella säkerhetspolitiska omgivning.

Under de senaste åren har skyddspolisen haft kontaktpersoner kortvarigt och långvarigt placerade vid de finska ambassaderna i vissa länder utanför Europa. Skyddspolisens kontaktpersoner deltar i avvärjningen av utländska hot mot statens säkerhet, bl.a. genom att upprätthålla kontakter till myndigheterna i stationeringslandet och i andra länder som är representerade där. Kontaktpersonernas verksamhet grundar sig på tillämpningen av bestämmelserna om polisens internationella informationsutbyte i lagen om behandling av personuppgifter i polisens verksamhet.

Den arbetsgrupp som utredde skyddspolisens administrativa ställning och resultatstyrning samt utvecklande av övervakningen framförde i sin slutrapport att det bör övervägas om skyddspolisens befogenheter för underrättelseinhämtning borde utvecklas. Av arbetsgruppens slutrapport framgår att den förändring i omvärlden som ligger till grund för behoven av befogenheter gäller framför allt Finlands yttre säkerhetspolitiska omgivning. Arbetsgruppens förslag, enligt vilket skyddspolisen för att bekämpa förehavanden som äventyrar rikets säkerhet bör kunna inhämta information med hjälp av verksamhet som gäller informationskällor, gäller också verksamhet utomlands.

Styrning av skyddspolisens verksamhet

I enlighet med 68 § 1 mom. i grundlagen, lagen om statsrådet (175/2003) och reglementet för statsrådet ska inrikesministeriet ansvara för de ministerieuppgifter som gäller polisen. Genom en ändring (860/2015) av polisförvaltningslagen överfördes skyddspolisen den 1 januari 2016 från att lyda under Polisstyrelsen till att bli en riksomfattande polisenhet under inrikesministeriet.

Skyddspolisens nya administrativa ställning framgår av 1 § 3 mom. i polisförvaltningslagen. Av det momentet och av 1 mom. i samma paragraf följer att inrikesministeriet ansvarar för styrningen och övervakningen av skyddspolisen och för sådana uppgifter inom skyddspolisens verksamhetsområde som enligt vad som föreskrivs särskilt ankommer på ministeriet. Enligt 5 § i statsrådets förordning om inrikesministeriet (1056/2013) bestäms i ministeriets arbetsordning förutom om ministeriets uppgifter och utövande av beslutanderätten också om styrning av ministeriets förvaltningsområde. Enligt 13 § (1562/2015) i den aktuella arbetsordningen behandlar polisavdelningen ärenden som gäller skyddspolisens verksamhet och resultatstyrningen av den.

I 10 § 1 mom. i polisförvaltningslagen anges förutom skyddspolisens uppgifter också att skyddspolisen omfattas av inrikesministeriets styrning. Med stöd av momentet fastställer inrikesministeriet exempelvis prioriteterna för inhämtande av information vid skyddspolisen (RP 346/2014 rd, s. 15). Genom att årligen fastställa prioriteterna styr inrikesministeriet skyddspolisens verksamhet genom att inrikta dess inhämtande av information. Fastställandet av prioriteterna för inhämtande av information vid skyddspolisen föregås av en förberedande behandling i utrikes- och säkerhetspolitiska ministerutskottet. I ett helhetsperspektiv handlar det således om en styr- och samordningsmekanism på statsrådsnivå. Det har inte utfärdats några lagbestämmelser om mekanismen.

Förutom för styrningen av skyddspolisens verksamhet ansvarar inrikesministeriet också för skyddspolisens resultatstyrning och tilldelningen av skyddspolisens resurser. Skyddspolisen har uppgifter som avviker från uppgifterna för polisen i övrigt, och därför behövs det för

skyddspolisen en uppsättning resultatmätare och en resursfördelningsmodell som avviker från det som gäller för polisen i övrigt; omkostnaderna för skyddspolisen har fått ett eget moment separat från omkostnadsmomentet för polisen. Dessutom skriver inrikesministeriet in preliminära resultatmål för skyddspolisen i statsbudgeten.

Inrikesministern bär politiskt ansvar för skyddspolisens verksamhet, och därför måste ministern känna till de centrala angelägenheterna inom ämbetsverkets verksamhetsområde. Följaktligen ska skyddspolisen underrätta inrikesministern om sådana angelägenheter i skyddspolisens uppgifter som är av samhällelig betydelse, och dessutom underrätta polisöverdirektören när angelägenheterna har betydande inverkan på det övriga polisväsendet. Skyddspolisens chef ska också hålla inrikesministeriet, närmare bestämt inrikesministern, kanslichefen och polisavdelningens överdirektör, informerat om angelägenheter som gäller skyddspolisen (RP 346/2014 rd, s. 15). Utöver att fullgöra anmälningsskyldigheten enligt 4 a § 2 mom. i polisförvaltningslagen ska skyddspolisen också med stöd av 10 § 3 mom. underrätta inrikesministeriet om sådana av skyddspolisen planerade förvaltningsinterna avgöranden eller förändringar i omständigheterna som på grund av sin beskaffenhet eller omfattning kan ha stor inverkan på realiseringen av de av inrikesministeriet godkända resultatmålen och riktlinjerna för skyddspolisen. Skyddspolisen informerar även republikens president, statsministern och utrikesministern samt riksdagens grundlags-, förvaltnings- och utrikesutskott för att de ska hålla sig à jour när det gäller utrikes- och säkerhetspolitiska angelägenheter och säkerhetsläget (RP 58/2009 rd, s. 20).

Enligt 10 § 4 mom. i polisförvaltningslagen kan inrikesministeriet i enskilda fall överta avgörandet av vissa av skyddspolisens förvaltningsinterna ärenden. Rätten att förbehålla sig beslutanderätten gäller för det första de resultatmål och riktlinjer som ministeriet har godkänt eller ärenden som inverkar på dem. Prioriteterna för inhämtande av information är riktlinjer som inrikesministeriet anvisat skyddspolisen, och därför kan förbehållandet av beslutanderätten gälla exempelvis prioriteterna eller ärenden som inverkar på dem. Till denna del handlar det om ett slags strategisk styrning i förhållandet mellan inrikesministeriet och skyddspolisen. För det andra inrymmer devolutionsrätten ärenden som gäller samarbetet eller arbetsfördelningen mellan skyddspolisen och de övriga polisenheterna. Med tanke på förvaltningsområdets interna problem har det för inrikesministeriet föreskrivits beslutanderätt i fråga om ärenden där skyddspolisen och Polisstyrelsen inte kan komma överens om ett avgörande. Ministern och i enskilda fall kanslichefen, chefen för en avdelning, chefen för en fristående enhet och chefen för en resultatenhet kan förbehålla sig beslutanderätten i ett ärende som en tjänsteman vid ministeriet annars skulle få avgöra (40 § i inrikesministeriets arbetsordning).

Laglighetsövervakning av skyddspolisens verksamhet

Rättslig grund för laglighetsövervakningen av skyddspolisen

Rättslig övervakning av civil underrättelseinhämtning behandlas i denna proposition till den del det finns bestämmelser om den i lagstiftningen om polisen. Övervakningen av underrättelseverksamheten samt laglighetsövervakningen av skyddspolisen granskas närmare i den proposition med förslag till lag om övervakning av underrättelseverksamheten som har samband med denna proposition.

Det finns inte något separat övervakningssystem för övervakning av skyddspolisens underrättelseverksamhet, utan underrättelseverksamheten övervakas på samma sätt som skyddspolisens övriga verksamhet. Skyddspolisen är en polisenhet som utövar polisens befogenheter, och laglighetsövervakningen av den har ordnats på samma sätt som laglighetsövervakningen av polisen i övrigt. Den 1 januari 2016 ändrades skyddspolisens administrativa ställning genom att skyddspolisen överfördes från att lyda under Polisstyrelsen till att bli en riksomfat-

tande polisenhet under inrikesministeriet. Polisstyrelsens ansvar för laglighetsövervakningen av skyddspolisen övertogs då av inrikesministeriet.

Laglighetsövervakning som inrikesministeriet genomför

Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag och ska lag iakttas noggrant i all offentlig verksamhet. Enligt 21§ i grundlagen har var och en rätt att på behörigt sätt och utan ogrundat dröjsmål få sin sak behandlad av en domstol eller någon annan myndighet som är behörig enligt lag samt att få ett beslut som gäller hans eller hennes rättigheter och skyldigheter behandlat vid domstol eller något annat oavhängigt rättskipningsorgan. Offentligheten vid handläggningen, rätten att bli hörd, rätten att få motiverade beslut och rätten att söka ändring samt andra garantier för en rättvis rättegång och god förvaltning ska tryggas genom lag. Enligt 22 § i grundlagen ska det allmänna se till att de grundläggande fri- och rättigheterna och de mänskliga rättigheterna tillgodoses. Enligt 68 § 1 mom. i grundlagen svarar varje ministerium inom sitt ansvarsområde för att förvaltningen fungerar som sig bör. Enligt 118 § 1 mom. i grundlagen svarar en tjänsteman för att hans eller hennes ämbetsåtgärder är lagliga. Enligt 2 mom. svarar en föredragande som inte har reserverat sig mot beslutet för det som har beslutats på föredragningen.

Enligt 14 § i statstjänstemannalagen (750/1994) ska en tjänsteman utföra sina uppgifter på behörigt sätt och utan dröjsmål. En tjänsteman ska också iaktta bestämmelserna om arbetsledning och övervakning. En tjänsteman ska uppträda så som hans eller hennes ställning och uppgifter förutsätter.

Enligt 4 § i polisförvaltningslagen ska Polisstyrelsen planera, utveckla, leda och övervaka polisverksamheten och dess stödfunktioner i fråga om polisenheterna under den. Enligt den ändring av 1 § i polisförvaltningslagen som trädde i kraft den 1 januari 2016 är skyddspolisen en riksomfattande enhet under inrikesministeriet.

I 5 kap. 63 § i polislagen finns bestämmelser om tillsyn över hemligt inhämtande av information. Enligt 1 mom. ska inhämtande av information enligt kapitlet övervakas av cheferna för de enheter som använder hemliga metoder för inhämtande av information, samt dessutom av inrikesministeriet när det är fråga om skyddspolisen och av Polisstyrelsen när det är fråga om en enhet som är underställd Polisstyrelsen. Enligt 2 mom. ska inrikesministeriet årligen till riksdagens justitieombudsman lämna en berättelse om hur hemliga metoder för inhämtande av information och skyddandet av dem har använts och övervakats. I 10 kap. 65 § 1 och 2 mom. finns motsvarande bestämmelser om hemliga tvångsmedel.

Inrikesministeriet riktar laglighetsövervakning särskilt till sådan verksamhet som det är svårast att nå med hjälp av extern kontroll och till ärenden som anknyter till de grundläggande fri- och rättigheterna samt de mänskliga rättigheterna. De centrala verksamhetsformerna för laglighetsövervakningen är att behandla förvaltningsklagan, medborgarbrev och egna initiativ, granskningar av laglighetsövervakningen och övervakning av behandlingen av personuppgifter.

Syftet med den interna laglighetsövervakningen är att övervaka att myndighetsverksamheten är lagenlig, att tjänsteåliggandena fullgörs och att anvisningarna följs. Laglighetsövervakningen tar fram korrekt samt så aktuell och tillräcklig information som möjligt om myndighetsverksamhetens lagenlighet för myndighetens ledning till stöd för beslutsfattandet. Laglighetsövervakningen bör sträva efter att förebygga eventuella fel samt avslöja felaktig eller lagstridig verksamhet i ett så tidigt skede som möjligt och underkasta den ändamålsenliga förfaranden.

Inrikesministeriets polisavdelning svarar vid inrikesministeriet för en ändamålsenlig organisering av laglighetsövervakningen av skyddspolisen. Chefen för skyddspolisen svarar för organiseringen av laglighetsövervakningen, tilldelningen av laglighetsövervakningens resurser och utvecklandet av laglighetsövervakningen vid skyddspolisen. Chefen för skyddspolisen ska se till att följande åtgärder vidtas vid skyddspolisen: regelbundna laglighetsgranskningar och övrig laglighetsövervakning enligt inrikesministeriets anvisning och skyddspolisens anvisningar. Den registeransvarige svarar för att personuppgifter behandlas lagenligt och att användningen övervakas.

Skyddspolisen utför regelbundna laglighetsgranskningar vid skyddspolisen baserade på en årlig plan. Skyddspolisen utarbetar årligen före utgången av februari en granskningsplan som fastställs av chefen för skyddspolisen och lämnas in till inrikesministeriets polisavdelning för kännedom.

Inrikesministeriets polisavdelning utför två granskningar av laglighetsövervakningen vid skyddspolisen baserade på den årliga planen. Granskningsberättelserna från inrikesministeriets polisavdelning och i synnerhet observationerna och åtgärdsrekommendationerna i dem behandlas av avdelningens ledningsgrupp. Chefen för polisavdelningen ska omedelbart informeras om betydande fel och brister samt lagstridig verksamhet. Behandlingen av granskningsobservationerna, åtgärderna och uppföljningen av åtgärderna ska dokumenteras.

Inrikesministeriets polisavdelning genomför sin laglighetsövervakning i enlighet med inrikesministeriets anvisning om intern laglighetsövervakning (SMDno-2016-329). Inrikesministeriets polisavdelning svarar för laglighetsövervakningen av skyddspolisen vid ministeriet. I inrikesministeriets anvisning om laglighetsövervakningen finns ett separat avsnitt om skyddspolisen. Inrikesministeriets polisavdelning utför årligen två granskningar vid skyddspolisen baserade på den årliga planen. I fråga om hemliga tvångsmedel och hemligt inhämtande av information iakttas, med vissa undantag, Polisstyrelsens föreskrift som gäller användning av i polislagen och tvångsmedelslagen avsedda hemliga metoder för inhämtande av information. Granskningsberättelserna lämnas in till riksdagens justitieombudsmans kansli för kännedom.

Intern laglighetsövervakning

Övervakningen vid skyddspolisen består av intern laglighetsövervakning, kvalitetskontroll och intern revision. Chefen för skyddspolisen svarar för organiseringen av laglighetsövervakningen, tilldelningen av laglighetsövervakningens resurser och utvecklandet av laglighetsövervakningen vid skyddspolisen. Chefen för skyddspolisen ska övervaka att följande åtgärder vidtas vid skyddspolisen: regelbundna laglighetsgranskningar och övrig laglighetsövervakning enligt inrikesministeriets anvisning om laglighetsövervakning och skyddspolisens egna anvisningar. Varje tjänsteman vid skyddspolisen, närcheferna och cheferna för resultatenheterna svarar för att verksamheten är lagenlig. Biträdande chefen, som leder den strategiska verksamheten, svarar för styrningen av laglighetsövervakningen. Den tjänsteman som förordnats för uppgiften svarar för de praktiska arrangemangen för laglighetsövervakningen.

Skyddspolisen utför regelbundna laglighetsgranskningar vid skyddspolisen baserade på en årlig plan. Det upprättas alltid en granskningsberättelse om granskningarna av laglighetsövervakningen. Inom skyddspolisens interna laglighetsövervakning fäster man särskild uppmärksamhet vid utövandet av befogenheter som kraftfullt ingriper i de grundläggande fri- och rättigheterna och de mänskliga rättigheterna, dvs. i synnerhet vid hemliga tvångsmedel och hemliga metoder för inhämtande av information (att formkraven iakttas, att lagstadgade anmälningar görs, att tidsfrister iakttas och att det görs dokumenteringar) samt behandlingen av personuppgifter och handlingar.

Tillsyn över hemliga tvångsmedel och över hemligt inhämtande av information

Det finns särskilda bestämmelser om tillsyn över polisens användning av hemliga tvångsmedel och hemligt inhämtande av information. Enligt 10 kap. 65 § i tvångsmedelslagen ska användningen av hemliga tvångsmedel vid polisen övervakas av cheferna för de enheter som använder sådana tvångsmedel och av Polisstyrelsen när det är fråga om en enhet som är underställd Polisstyrelsen. När det är fråga om skyddspolisen övervakar inrikesministeriet användningen av hemliga tvångsmedel. I 5 kap. 63 § i polislagen finns bestämmelser om tillsyn över hemligt inhämtande av information Enligt paragrafen ska inhämtande av information enligt 5 kap. i polislagen övervakas av cheferna för de enheter som använder hemliga metoder för inhämtande av information samt av Polisstyrelsen när det är fråga om en enhet som är underställd Polisstyrelsen. När det är fråga om skyddspolisen övervakar inrikesministeriet verksamheten. Inrikesministeriet ska årligen lämna riksdagens justitieombudsman en berättelse om hur hemliga tvångsmedel och skyddandet av dem har använts och övervakats samt om hur hemliga metoder för inhämtande av information och skyddandet av dem har använts och övervakats. I polislagen föreskrivs det om de berättelser om hemligt inhämtande av information för att förhindra och avslöja brott som ska lämnas till justitieombudsmannen.

Bestämmelser om övervakning av hemligt inhämtande av information finns dessutom i 3 kap. 21 § i statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information (122/2014). Enligt paragrafen ska Polisstyrelsen tillsätta en grupp för övervakning av användningen av hemliga tvångsmedel och hemliga metoder för inhämtande av information. Till medlemmar i gruppen kan förordnas företrädare för Polisstyrelsen, centralkriminalpolisen, skyddspolisen och polisinrättningen. Till medlemmar i gruppen kallas en representant för inrikesministeriet, en av staben för gränsbevakningsväsendet utsedd representant för gränsbevakningsväsendet, en av huvudstaben utsedd representant för försvarsmakten och en representant för Tullen. Enligt 2 mom. har gruppen till uppgift att övervaka verksamhet, samarbete och utbildning, behandla omständigheter som framkommit i verksamheten och samarbetet eller som är viktiga för laglighetsövervakningen samt att rapportera dessa omständigheter till Polisstyrelsen, lägga fram förslag om hur verksamheten ska utvecklas, samt samordna beredningen av de berättelser som ska lämnas till riksdagens justitieombudsman.

Skyddspolisen iakttar Polisstyrelsens föreskrift om organisering, nyttjande och övervakning av hemligt inhämtande av information (POL-2014-3305) med vissa preciseringar. Vid skyddspolisen har man bl.a. bildat ett system med ansvariga personer i enlighet med föreskriften. De ansvariga personerna övervakar med framförhållning och i realtid hemliga tvångsmedel och hemligt inhämtande av information. De tvångsmedelsdokumenteringar som görs i systemen inom ramen för de arrangemang som utformats och deras rättsliga grund granskas i realtid. Dessutom granskar skyddspolisens laglighetsövervakare hemliga tvångsmedel och hemliga metoder för inhämtande av information på ett övergripande sätt en gång i halvåret.

2.3 Den internationella utvecklingen och lagstiftningen i utlandet

Allmänt

I avsnittet med den internationella jämförelsen behandlas lagstiftningen om civil och militär underrättelseinhämtning i Norge, Danmark och Tyskland ämnesvis. I försvarsministeriets proposition som gäller lagstiftningen om militär underrättelseverksamhet och som har samband med den här propositionen behandlas på motsvarande sätt lagstiftningen i Sverige, Holland och Schweiz. Den rättsliga och parlamentariska övervakningen av jämförelsestaternas underrättelseinhämtning behandlas i justitieministeriets proposition om övervakning av underrättelseverksamheten som har samband med den här propositionen.

Genom underrättelseinhämtningen skyddas den nationella säkerheten. Den nationella säkerheten har av tradition ansetts vara en del av kärnan i staternas suveränitet. Trots detta begränsar internationella människorättskonventioner hur staterna i sin nationella lagstiftning får reglera den nationella säkerheten och underrättelseinhämtningen.

Under de senaste åren har de ekonomiska satsningarna på underrättelsetjänsternas verksamhet ökat betydligt i de jämförelseländer som behandlas härnäst i och med att säkerhetsförhållandena har förändrats. I till exempel Danmark ökade budgeten för polisens säkerhetstjänst PET (Politiets Efterretningstjeneste), som ansvarar för avvärjande av inre säkerhetshot, med 43 procent mellan 2013 och 2017 och uppgick under 2017 till 107 miljoner euro, medan budgeten för försvarets underrättelsetjänst FE (Forsvarets Efterretningstjeneste), som ansvarar för informationsinhämtning som avser utländska förhållanden, under samma tidsperiod steg med 42 procent till 118 miljoner euro. Under detta år lägger Danmark således sammanlagt 225 miljoner euro på sina säkerhets- och underrättelsetjänsters verksamhet. Enligt offentliga uppgifter ökade budgeten för Tysklands civila säkerhetstjänst på förbundsstatsnivå, Bundesverfassungsschutz (BfV), med cirka 60 procent till 349 miljoner euro mellan 2014 och 2017 och budgeten för underrättelsetjänsten som avser utländska förhållanden, Bundesnachrichtendienst (BND), ökade med 35 procent till 833 miljoner euro och budgeten för Militärischer Abschirmsdienst (MAD) till 3,8 miljoner euro under samma tid. År 2017 finansierar Tyskland säkerhets- och underrättelsetjänsternas verksamhet på förbundsstatsnivå med sammanlagt 1,4 miljarder euro. I denna summa ingår inte utgifterna för delstaternas säkerhetstjänster. I Tyskland har också var och en av de sexton delstaterna en egen säkerhetstjänst.

Norge

I Norge är det Etterretningstjenesten (E-tjenesten) som är den underrättelsetjänst som avser utländska förhållanden och dess uppgifter och befogenheter regleras i en lag och en förordning om underrättelsetjänsten (Lag om Etterreningstjenesten, Instruks om Etterretningstjenesten). Norge har ingen säkerhetstjänst inom landet, utan för landets inre, nationella säkerhet svarar säkerhetspolisen Politiets sikkerhetstjeneste (PST). Samarbetet mellan E-tjenesten och PST regleras i en egen förordning (Instruks om samarbejdet mellom Etteretningstjenesten og Politiets sikkerhetstjeneste).

Styrning

Underrättelsetjänsten är en del av det norska försvaret. Chefen för underrättelsetjänsten står direkt under chefen för försvarsmakten. Chefen för underrättelsetjänsten är rådgivare för chefen för försvarsmakten i ärenden som gäller underrättelseverksamhet.

För den politiska styrningen av underrättelsetjänsten och övervakningen av verksamheten svarar försvarsministeriet. Underrättelsetjänsten informerar ministeriet om sin verksamhet och får uppdrag av ministeriet. Styrningen, övervakningen och rapporteringen sker via chefen för försvarsmakten.

Underrättelsetjänsten är skyldig att lägga fram vissa viktiga ärenden för försvarsministeriet för beslut. Sådana ärenden som ministeriet fattar beslut om är etablering av samarbete med nya internationella samarbetspartner, organisering av ockupationsberedskap, inledande av politiskt känsliga så kallade särskilda underrättelseoperationer samt andra ärenden som är särskilt viktiga eller av principiell karaktär.

De andra ministerierna och myndigheter får med tillstånd av försvarsministeriet ge underrättelsetjänsten uppdrag.

Underrättelsetjänstens uppgift

Underrättelsetjänstens allmänna uppgift är att inhämta, bearbeta och analysera information om norska intressen i förhållande till främmande stater, organisationer och individer och utarbeta hotbilds- och underrättelsebedömningar för att trygga viktiga nationella intressen. Lagen innehåller en förteckning över nationella intressen som ska tryggas. Till dem hör bland annat utformningen av norsk utrikes-, försvars- och säkerhetspolitik, beredskapsplaneringen och strukturutvecklingen av försvaret samt tillhandahållandet av information om internationell terrorism, gränsöverskridande miljöproblem och massförstörelsevapen. Förteckningen är inte uttömmande och de nationella intressen som underrättelsetjänsten skyddar vid varje tidpunkt är beroende av förändringar som sker i de norska säkerhetsförhållandena. Enligt förordningen om underrättelsetjänsten är huvuduppgiften dock att inhämta sådan information om andra länders politiska och samhälleliga utveckling, intentioner och militära styrka som kan utgöra ett hot för Norges säkerhet. Enligt förordningen är en prioriterad uppgift att ge underrättelsestöd till norska enheter som deltar i internationella militära operationer. Om den centrala prioriteringen vid civila mål för underrättelseinhämtningsuppgifter beslutar försvarsministeriet efter att ha förhandlat om detta med underrättelsetjänsten och andra myndigheter som behöver underrättelseinformation.

Metoder för informationsinhämtning och beslut om att de ska användas

Det finns inga bestämmelser om metoderna för underrättelsetjänstens informationsinhämtning eller om de metoder som den använder för personbaserad underrättelseinhämtning och teknisk underrättelseinhämtning. Av lagstiftningen kan man endast indirekt dra slutsatsen att underrättelsetjänsten över huvud taget kan använda sig av hemliga metoder för informationsinhämtning. Förordningen om underrättelsetjänsten kompletterades 2013 med bestämmelser om förutsättningarna för insamling av information om norska personer i utlandet. Bestämmelserna i sig preciserar inte metoderna för insamling av information, utan de sätter gränser för i vilket syfte och under hurdana förhållanden som information om norska medborgare i utlandet får samlas in. Enligt definitionen av insamling av information i de kompletterande bestämmelserna avses med insamling av information ”övervakning och annan hemlig informationsinhämtning”. Det går också att dra slutsatsen att hemlig informationsinhämtning förekommer utifrån bestämmelserna i förordningen om samarbete mellan underrättelsetjänsten och polisens säkerhetstjänst. Enligt dessa ska parterna utbyta information om utvecklingen av teknologier och metoder samt ge varandra stöd i fråga om utrustning och teknik i konkreta operationer för informationsinhämtning. För användningen av hemliga metoder för informationsinhämtning talar också det att underrättelsetjänsten är förpliktad att överlåta beslutsfattandet om politiskt känsliga särskilda operationer för underrättelseinhämtning till ministeriet.

Rapportering

Underrättelsetjänsten ska informera försvarsministeriet och efter beslut av försvarsministeriet andra berörda ministerier om ändringar i de norska yttre säkerhetsförhållandena. För direktrapportering till uppdragsgivare utanför försvarsförvaltningen krävs tillstånd av försvarsministeriet.

Samarbete med brottsbekämpande myndigheter

Det finns inga konkreta bestämmelser om utlämnande av den information som underrättelsetjänsten inhämtat för att förebygga, avslöja eller utreda brott. Det har dock utfärdats en egen förordning om samarbetet mellan underrättelsetjänsten och polisens säkerhetstjänst. Polisens säkerhetstjänst har till uppgift att förebygga, avslöja och utreda vissa brott som är riktade mot den nationella säkerheten.

I förordningen anges att prioriterade samarbetsområden för ömsesidigt informationsutbyte och annat samarbete utgörs av bekämpning av terrorism, spridning av massförstörelsevapen och olaglig underrättelseverksamhet och andra prioriterade förhållanden som gäller viktiga norska intressen. Parterna ska också bistå varandra såväl i konkreta operationer för informationsinhämtning och i utbyte av operativ information som i analyseringen av strategisk information och hotbildsbedömningar. Samarbetsformerna omfattar också ömsesidigt tekniskt stöd och utbildningsstöd mellan parterna, tjänstemannautbyte och internationell kontaktpersonsverksamhet. En förutsättning för samarbetet är att parterna följer bestämmelserna om de egna befogenheterna. Normalt är det cheferna för tjänsterna som fattar beslut om begäran om och beviljande av stöd vid operationer för informationsinhämtning. I särskilt viktiga ärenden är det dock ministerierna som styr tjänsternas verksamhet.

Samarbetsförordningen förpliktar parterna att utbyta så kallad överskottsinformation. Med överskottsinformation avses information som inte gäller ifrågavarande tjänsts ansvarsområde, men som tjänsten fått i samband med informationsinhämtningen. Överskottsinformationen kan utgöras av personuppgifter till exempel om personer i utlandet som äventyrar norska intressen. Den part som lämnar ut överskottsinformationen kan kräva att mottagaren inte lämnar informationen vidare utan samtycke från den som lämnat ut den. Enligt förordningen om underrättelsetjänsten får underrättelsetjänsten lämna ut överskottsinformation om personer som den fått i samband med sin informationsinhämtning också till andra norska myndigheter än polisens säkerhetstjänst.

Underrättelsetjänsten får inte på norskt territorium förtäckt inhämta information om norska medborgare eller norska juridiska personer. Som ett undantag från detta får underrättelsetjänsten dock förtäckt inhämta information om sådana norska personer som vistas i Norge som deltar i olaglig underrättelseverksamhet för en främmande stats räkning. I detta fall ska underrättelsetjänstens informationsinhämtning ske via polisens säkerhetstjänst eller med dess tillstånd.

Det finns inga bestämmelser om samarbete mellan underrättelsetjänsten och öppna polisen. Av samarbetsförordningen framgår dock indirekt att sådant samarbete förekommer, eftersom förordningen enligt bestämmelserna om förordningens tillämpningsområde inte ska tillämpas på underrättelsetjänstens stöd eller utlämnande av uppgifter till tullmyndigheterna eller öppna polisen. Enligt förordningen får sådant utlämnande av information dock kanaliseras via polisens säkerhetstjänst. Underrättelsetjänsten kan genom polisens säkerhetstjänst ställa villkor för vad den polisenhet som är den slutliga mottagaren får använda uppgifterna till samt kräva att polisens säkerhetstjänst inte avslöjar att uppgifterna kommer från underrättelsetjänsten.

Internationellt samarbete

Enligt lagen om underrättelsetjänsten får underrättelsetjänsten etablera och upprätthålla underrättelsesamarbete med andra länder. Försvarsministeriet beslutar om att samarbetsrelationer ska inledas med nya samarbetspartner på förslag av underrättelsetjänsten. Underrättelsetjänsten och polisens säkerhetstjänst ska koordinera sina internationella samarbetsrelationer.

År 2013 fogades kompletterande bestämmelser till förordningen om underrättelsetjänsten och de gäller under vilka förutsättningar underrättelsetjänsten får lämna ut personuppgifter om norska medborgare till utländska underrättelsetjänster. Uppgifterna får lämnas ut om detta sker i enlighet med underrättelsetjänstens lagstadgade uppgifter och underrättelsetjänsten har rätt att lagra uppgifterna i sitt personregister. Dessutom krävs att utlämnandet sker i norskt intresse, att det bedöms vara nödvändigt efter övervägande av förhållandet mellan att skydda viktiga nationella intressen och konsekvenserna för personen som det lämnas ut uppgifter om och att utlämnandet är försvarligt med beaktande av uppgifternas karaktär, vem de handlar om och vem som tar emot dem. För utlämnandet av uppgifterna ställs villkoret att uppgifterna inte

får användas som grund för hemlig informationsinhämtning riktad mot personer som vistas på norskt territorium. De här kraven tillämpas endast vid utlämnandet av personuppgifter om norska medborgare. Det har inte ställts några villkor för utlämnande av uppgifter om utländska medborgare.

Ett lagstiftningsprojekt om underrättelseinhämtning som avser datatrafik

I februari 2016 tillsatte Norges försvarsminister en kommitté för bedömning av behovet av lagstiftning om underrättelseinhämtning som avser datatrafik. Kommittén överlämnade sitt betänkande (Digitalt grenseforsvar (DGF). Lysne II-utvalget. 26 August 2016) till försvarsministern i september samma år.

I betänkandet föreslog kommittén att det ska lagstiftas om underrättelseinhämtning som avser datatrafik, eftersom det enligt den handlar om nödvändiga befogenheter för att skydda det demokratiska samhället och den nationella säkerheten. Enligt kommittén borde befogenheten ges till E-tjeneste för informationsinhämtning om bland annat allvarliga cyberhot, terrorism och spionage riktat mot Norge. Användningsändamålen borde vara bundna till E-tjenestens uppgifter och också motsvara de underrättelseprioriteringar som regeringen årligen anvisar underrättelsetjänsten. Prioriteringarna inom underrättelseinhämtningen är inte offentliga och därmed är det inte känt om informationsinhämtningen till sin karaktär är baserad endast på hot eller mer omfattande än detta.

Kommittén föreslog att den underrättelseinhämtning som avser datatrafik ska gälla filtrering av datatrafik i kablar som korsar Norges gränser med hjälp av sökbegrepp. Det ska vara tillåtet att använda både innehållsbeskrivande sökbegrepp och andra sökbegrepp i verksamheten, men krävas förhandstillstånd av en domstol. Enligt kommitténs inställning ska all eventuell så kallad överskottsinformation som kommer fram i verksamheten utplånas. Därmed kan endast sådan information bevaras som direkt hör samman med E-tjenestens uppgifter och de underrättelseprioriteringar som regeringen anvisat E-tjenesten. Kommittén tog inte ställning till utlämnande av sådan information till polismyndigheterna, men konstaterade att användning av information från underrättelseinhämtning som avser datatrafik som bevis i rättegångar under inga omständigheter får tillåtas.

Enligt kommittén kan sådan underrättelseinhämtning som avser datatrafik som det föreskrivs tillräckligt noggrant om på lagnivå bidra till att förbättra verksamhetsförutsättningarna för näringslivet i Norge. Kommittén förkastade uppfattningen att Norge borde kvarstå som en ”övervakningsfri zon” för att locka till internationella investeringar. En tillräckligt exakt och öppen lagstiftning i kombination med en klar förmåga från underrättelsemyndigheternas sida till att skydda Norge mot yttre cyberangrepp kan tvärtom stärka Norges internationella konkurrensförmåga och attraktionskraft som investeringsobjekt.

Kommittén bedömde också att det är möjligt att föreskriva om underrättelseinhämtning som avser datatrafik på ett sätt som är förenligt med de internationella människorättsförpliktelser som Norge är bundet till genom den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och tolkningspraxisen inom EU-rätten. Detta förutsätter att det i en eventuell lag om underrättelseinhämtning som avser datatrafik tillräckligt tydligt föreskrivs om användningsgrunderna för underrättelseinhämtningen som avser datatrafik och om hanteringen av de uppgifter som inhämtats med hjälp av den samt om rättsskyddsmekanismerna. Kommittén föreslog att rättsskyddsarrangemangen kring underrättelseinhämtning som avser datatrafik ska fungera både på förhand och i efterhand. Rättsskyddet genomförs på förhand genom lagstiftning om att en domstol ska fatta beslut om att underrättelseinhämtning som avser datatrafik får användas. Det krävs att en domstol godkänner användningen av sådana sökbegrepp som beskriver innehållet i ett meddelande

vid filtreringen. De metadata som samlas in i samband med underrättelseinhämtningen som avser datatrafik lagras i ett datalager som skapas för just detta ändamål och domstolen godkänner att sökningar görs i det. Enligt kommittén är det önskvärt att domstolen är insatt i underrättelseverksamhetens verksamhetsmiljö, E-tjenestens verksamhet och tekniska frågor och att antalet ledamöter är tillräckligt begränsat av sekretesskäl. Detta kan motivera att en specialdomstol inrättas.

För att säkerställa rättsskyddet i efterhand bedömde kommittén att det är behövligt att stärka både laglighetsövervakningen och delvis också den parlamentariska övervakningen. Enligt kommittén bör ett nytt organ för laglighetsövervakningen av underrättelseinhämtningen som avser datatrafik inrättas (”DGF-tilsynet”), och det ska få uppgifter bland annat om alla sökningar som gjorts i metadatalagret, de tillstånd som beviljats av domstol för underrättelseinhämtning som avser datatrafik och verkställandet av dem samt om konfigurationen av de filter som används inom underrättelseinhämtningen som avser datatrafik. Utskottet EOS-utvalget som i enlighet med vad som konstaterats ovan inte kan ses som ett rent parlamentariskt kontrollorgan ska kunna övervaka underrättelseinhämtningen som avser datatrafik på samma sätt som det övervakar E-tjenestens övriga verksamhet. DGF-tilsynet ska åläggas att lämna sin rapport till utskottet och utskottet ska ha begränsad tillgång till de informationssystem som gäller underrättelseinhämtningen som avser datatrafik. EOS-utvalget ska rapportera till Stortinget om användningen av underrättelseinhämtning som avser datatrafik liksom om den styrning som försvarsministeriet riktar mot denna underrättelseinhämtning.

I betänkandet finns en detaljerad analys av EU-domstolens senaste rättsfall. Enligt riktlinjerna ovan bedöms den genomförda underrättelseinhämtningen som avser datatrafik vara förenlig med de rättsnormer som ingår i de avgöranden som getts i de fall som också behandlas i denna proposition Digital Rights Ireland m.fl. (C-293/12) och Schrems (C-362/14). Avgörandena anses i alla fall vara tillämpliga endast delvis på underrättelseinhämtning som avser datatrafik.

I betänkandet finns en nationell jämförelse som är mer omfattande om också mer generell än den som ingår i denna regeringsproposition. Jämförelsestaterna utgörs av Sverige, Frankrike, Förenade kungariket, Kanada, Tyskland, Nederländerna, Schweiz och Finland. Kommittén konstaterar att den utgår från att många sådana länder som inte har någon lagstiftning om underrättelseinhämtning som avser datatrafik använder sig av sådan trots avsaknaden av rättsgrunden för detta. Enligt kommittén utgör såväl iakttagande av de mänskliga rättigheterna som förutsägbarhet inom de ekonomiska förhållandena motiv för en öppen och exakt lagstiftning i ärendet.

Av betänkandet framgår att den norska nationella säkerhetsmyndigheten kontrollerar ett nationellt observationssystem för kränkningar av informationssäkerheten som är baserat på filtrering. Av beskrivningen av observationssystemet i betänkandet kan man dra slutsatsen att systemet till sina verksamhetsprinciper motsvarar Kommunikationsverkets så kallade HAVARO-system, som behandlas senare i den här propositionen. Enligt betänkandet är observationssystemets möjligheter att identifiera allvarligare cyberhot mot Norge otillräckliga, varför lagstiftning om underrättelseinhämtning som avser datatrafik är nödvändig för att skydda sig mot hoten.

Danmark

Styrning

Försvarets underrättelsetjänst FE är trots sitt namn inte en del av försvaret utan en civil myndighet, som lyder under och styrs av Danmarks försvarsministerium. Försvarsministern kan

anvisa sådana uppgifter till underrättelsetjänsten som har samband med dess lagstadgade ansvarsområde.

Underrättelsetjänstens uppgift

I lagen föreskrivs att FE:s uppgifter är att tillhandahålla den underrättelsemässiga grunden för dansk utrikes-, säkerhets- och försvarspolitik, medverka till att förebygga och motverka hot mot Danmark och danska intressen och i samband med detta inhämta, analysera och rapportera uppgifter om sådana förhållanden i utlandet som är av betydelse för Danmark och danska intressen i utlandet. FE är också Danmarks så kallade nationella säkerhetsmyndighet och nationella myndighet för informationssäkerhet.

Metoder för informationsinhämtning och beslut om att de ska användas

Det finns ingen egentlig reglering av de konkreta metoder för informationsinhämtning som underrättelsetjänsten använder eller av villkoren för att metoderna ska få användas. Enligt lagen om försvarets underrättelsetjänst kan FE samla in och inhämta information som är av betydelse för dess underrättelseverksamhet. Enligt förarbetena till lagen har tröskeln för informationsinhämtning medvetet satts lågt. Det är en ytterst viktig uppgift för underrättelsetjänsten att upptäcka nya okända säkerhetshot. I sådana fall är det inte möjligt att specificera föremålet för informationsinhämtningen i det skede när denna verksamhet inleds. Bestämmelsen om informationsinhämtning är enligt förarbetena formulerad så att den gör det möjligt att inhämta ytterst stora mängder information.

I lagen anges inte underrättelsetjänstens olika metoder för underrättelseinhämtning. Enligt offentliga källor inhämtas information såväl som inhämtning av personuppgifter med hjälp av signalspaning elektroniskt från satelliter och datatrafikkablar som via öppna källor.

På samma sätt som i Norge har man i Danmark också nyligen föreskrivit om förutsättningarna för att få inhämta information om sådana medborgare i det egna landet som vistas utomlands. Information om i Danmark hemmahörande fysiska och juridiska personer som vistas utomlands får inhämtas om det finns grundad anledning att anta att personen deltar i verksamhet som utgör ett terrorhot mot Danmark eller danska intressen. Om informationsinhämtningen förutsätter ingripande i skyddet av förtroliga meddelanden måste tillstånd sökas hos domstol. I ansökan om tillstånd ska det ingå uppgifter om den person eller de personer som är föremål för informationsinhämtningen samt om de förhållanden utifrån vilka det finns fog att anta att personerna i fråga deltar i verksamhet som utgör ett terrorhot mot Danmark eller danska intressen.

Tillståndsförfarandet tillämpas endast då informationsinhämtningen riktas mot en dansk medborgare. Ingripande i konfidentiell kommunikation i fråga om utländska fysiska eller juridiska personer kräver inget tillstånd av domstol.

Rapportering

Underrättelsetjänsten ska inom ramen för sitt ansvarsområde hålla försvarsministeriet kontinuerligt underrättat om förhållanden som är av betydelse för Danmark och danska intressen och förhållanden som är av väsentlig betydelse för underrättelsetjänstens egen verksamhet. Dessutom ska den informera ministeriet om de mest betydande enskilda ärendena som det hanterar. Det finns inga andra bestämmelser som gäller rapportering.

Samarbete med brottsbekämpande myndigheter

Polisens säkerhetstjänst PET ansvarar för förebyggande, avslöjande och utredande av brott som äventyrar den nationella säkerheten, bland annat terrorbrott samt högförräderi- och landsförräderibrott.

Underrättelsetjänsten och polisens säkerhetstjänst får lämna ut personuppgifter och annan information till varandra om detta kan vara av betydelse för skötseln av någonderas uppgifter. Syftet är att parterna inte i varje enskilt fall särskilt ska behöva bedöma om utlämnandet av information är nödvändigt. Enligt ett statligt betänkande med förslag till lagar om FE och PET är tjänsternas uppgifter så nära knutna till varandra att utlämnande av information mellan dem i hög grad kan jämställas med internt utlämnande av information inom en myndighet.

Underrättelsetjänsten får lämna ut information om danska medborgare till andra polisenheter än polisens säkerhetstjänst om detta kan vara av betydelse för skötseln av underrättelsetjänstens egna lagstadgade uppgifter. På samma grunder kan den lämna ut sådan information till andra danska myndigheter.

Internationellt samarbete

I lagen finns inga bestämmelser om underrättelsetjänstens internationella samarbete. I förarbetena till lagen konstateras att Danmark är ett litet land som är helt beroende av information från utländska samarbetspartner, varför underrättelsetjänsten måste arbeta i nära operativt samarbete med säkerhets- och underrättelsetjänster i andra stater. Underrättelsetjänstens rätt att lämna ut information om danska medborgare till andra stater och internationella organisationer är begränsad genom att utlämnandet av information ska vara av betydelse för skötseln av underrättelsetjänstens egna lagstadgade uppgifter. Information kan således lämnas ut till utlandet på samma villkor som till danska myndigheter.

Tyskland

I Tyskland är Bundesnachrichtendienst (BND) den underrättelsetjänst som avser utländska förhållanden och den svarar för den externa informationsinhämtningen som gäller både civila och militära hot. Säkerhetstjänsten inom landet är indelad så att Bundesverfassungsschutz (BfV) är förbundsstatens civila säkerhetstjänst och Militärischer Abschirmsdienst (MAD) den militära säkerhetstjänsten. Alla de här aktörernas uppgifter och befogenheter regleras i egna lagar, även om de lagar som gäller BND:s och MAD:s verksamhet i fråga om befogenheterna i stor utsträckning hänvisar till lagen om BfV:s verksamhet. Med tanke på regleringen av befogenheterna är också lagen om begränsande av post- och telehemligheten (G10-lagen, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses), av stor betydelse och i den finns bestämmelser om alla sådana metoder för underrättelseinhämtning som säkerhets- och underrättelsetjänsterna får använda för att ingripa i innehållet i förtroliga meddelanden i sin informationsinhämtning.

Tyskland är en förbundsstat och förbundsstaten och delstaterna har delad befogenhet i ärenden som gäller inrikesfrågor. Av detta följer att det i Tyskland vid sidan av förbundsstatens civila säkerhetstjänst BfV finns en egen civil säkerhetstjänst (Landesverfassungsschutz) i varje delstat. Emedan utrikes- och försvarsärenden hör uteslutande till förbundsstatens befogenhet, har delstaterna inga egna underrättelsetjänster som avser utländska förhållanden eller militära säkerhetstjänster.

Styrning

Underrättelsetjänsten som avser utländska förhållanden, BND, lyder under och styrs av förbundskanslersämbetet. För styrningen svarar en underrättelsekoordinator vid förbundskanslersämbetet. På motsvarande sätt lyder förbundsstatens civila säkerhetstjänst BfV under och styrs av förbundsstatens inrikesministerium och den militära säkerhetstjänsten MAD lyder under och styrs av förbundsstatens försvarsministerium. Delstaternas säkerhetstjänster är inte underställda förbundsstatens säkerhetstjänst, utan var och en lyder under den egna delstatens inrikesministerium. Till följd av den delade befogenheten föreskrivs det separat om samarbetet mellan förbundsstatens säkerhetstjänst och delstaternas säkerhetstjänster.

Det finns inga närmare bestämmelser i lagen om ministeriernas styrningsbehörigheter. I lagen föreskrivs det inte om förutsättningarna för och beslutsförfarandena kring användningen av andra hemliga metoder för informationsinhämtning än dem som ingriper i skyddet för förtroliga meddelanden. Om dem finns i stället bestämmelser i underrättelse- och säkerhetstjänsternas reglementen som utfärdas av de ministerier som ansvarar för verksamheten. Utfärdandet av reglementena, som är sekretessbelagda, kan i sig anses vara en viktig form av styrningsbehörighet. Dessutom kan man anta att reglementena innehåller närmare bestämmelser för hur säkerhets- och underrättelsetjänsterna styrs rent konkret.

Observera att en form av styrning innebär att de ministerier som svarar för säkerhets- och underrättelsetjänsternas verksamhet deltar i beslutsfattandet om användningen av hemliga metoder för informationsinhämtning som ingriper i skyddet för förtroliga meddelanden. Det styrande ministeriet godkänner till exempel på förhand ansökningarna om teleavlyssning och underrättelseinhämtning som avser datatrafik innan de – beroende på metoden för informationsinhämtning – styrs vidare till tillståndsförfarandet vid myndigheten för laglighetsövervakning eller myndigheten för parlamentarisk övervakning.

Underrättelsetjänstens uppgift

BND:s uppgift är enligt lagen att inhämta och analysera underrättelseinformation som är av betydelse för Tysklands utrikes- och säkerhetspolitik. En allmän förutsättning för inhämtande av information om händelser i utlandet av utrikes- och säkerhetspolitisk betydelse är att den inte kan inhämtas på något annat sätt och att ingen annan myndighet ansvarar för att inhämta den.

BfV:s och delstaternas säkerhetstjänsters lagstadgade uppgift är att inhämta och analysera underrättelseinformation om verksamhet som strider mot den demokratiska samhällsordningen och grundlagsordningen liksom om verksamhet som äventyrar förbundsstatens och delstaternas existens och säkerhet. Dessutom ska de inhämta och analysera information om underrättelseverksamhet och annan verksamhet som hotar Tysklands säkerhet och som utövas för en främmande makt, våldsamma försök att äventyra tyska externa säkerhetsintressen samt försök att motarbeta det internationella samförståndet eller den fredliga samexistensen mellan olika folk. Sammanslutningar som främjar sådana försök är förbjudna i den tyska grundlagen som stiftades efter slutet av det andra världskriget.

Den militära säkerhetstjänsten MAD inhämtar och analyserar underrättelseinformation om likartade hot som BfV, dock under förutsättning att hoten är riktade mot personal, enheter och inrättningar inom försvarsministeriets förvaltningsområde och att en anställd inom försvarsministeriets förvaltningsområde ligger bakom hotet. Dessutom är det MAD:s uppgift att inhämta och analysera information om personal inom försvarsministeriets förvaltningsområde som eventuellt deltar i försök att motarbeta det internationella samförståndet eller den fredliga samexistensen mellan olika folk. MAD:s primära uppgift är således att upptäcka och avvärja

hot som uppkommer inom Tysklands försvarsförvaltning. Dessutom är dess uppgift att bedöma säkerhetsläget för enheter och baser som är underställda försvarsförvaltningen liksom Natos baser som är placerade i Tyskland, oberoende av varifrån hotet kommer. För den sistnämnda uppgiften finns inga särskilda befogenheter för informationsinhämtning, utan det är fråga om analysering av uppgifter som kommit från andra aktörer.

Metoder för informationsinhämtning och beslut om att de ska användas

I den tyska lagstiftningen är underrättelse- och säkerhetstjänsternas hemliga underrättelseinhämtningsmetoder indelade i sådana som inte ingriper i innehållet i förtroliga meddelanden, som är särskilt skyddat i Tysklands grundlag, och sådana som gör det. Det föreskrivs om de så kallade allmänna underrättelseinhämtningsmetoderna, som hör till den förstnämnda gruppen, i speciallagar som gäller underrättelse- och säkerhetstjänsternas verksamhet och i de reglementen som de styrande ministerierna har utfärdat för de tjänster som lyder under dem. Om den senare gruppen, det vill säga de underrättelseinhämtningsmetoder som ingriper i innehållet i förtroliga meddelanden, föreskrivs det gemensamt för alla tjänster i den så kallade G10-lagen.

I 8 § i BfV-lagen finns en grundläggande bestämmelse som gäller användningen av allmänna underrättelseinhämtningsmetoder. Enligt den får säkerhetstjänsten dra nytta av sådana hemliga metoder för informationsinhämtning som användning av medhjälpare som handleds av säkerhetstjänsten, infiltrering, teknisk observation och avlyssning, användning av falska dokument och registreringsskyltar, om de behövliga uppgifterna inte kan inhämtas på något mindre integritetsingripande sätt. Den förteckning över hemliga informationsinhämtningsmetoder som finns i bestämmelsen utgör endast exempel. Konkretare bestämmelser om metoderna för informationsinhämtning samt förutsättningarna för och beslutsfattandet kring användningen av metoderna finns i BfV:s reglemente, som förbundsstatens inrikesminister godkänner och lämnar för kännedom till det parlamentariska kontrollorganet. BfV:s reglemente är inte en offentlig handling.

I 8a § och 9 § i BfV-lagen finns några specialbestämmelser om säkerhetstjänstens rätt att få information och tekniska metoder för informationsinhämtning. Den första bestämmelsen gäller BfV:s rätt att få kunduppgifter av flygbolag, banker och andra finansinstitut, företag som tillhandahåller posttjänster och teletjänstleverantörer oberoende av de sekretessbestämmelser som dessa är bundna av. Även så kallade retroaktiva teleövervakningsuppgifter omfattas av rätten att få information. För begäran av uppgifter av post- och teleföretag krävs ett beslut av chefen för BfV eller dennes vikarie, medan beslut om begäran av resenärs- och bankuppgifter fattas på lägre nivå. Enligt 9 § i BfV-lagen får säkerhetstjänsten rikta hemlig avlyssning och observation mot ett utrymme som används för boende endast om detta är nödvändigt för att avvärja en omedelbar fara och när polisen inte hinner vidta åtgärder i tid. Beslutet om avlyssning eller observation av en bostad fattas av chefen för säkerhetstjänsten eller dennes vikarie och det rättsliga avgörandet träffas av tingsrätten. I 9 § i BfV-lagen finns också reglering som gäller positionsbestämning av mobiltelefoner.

I lagarna om BND:s och MAD:s verksamhet hänvisas i bestämmelserna om de allmänna metoderna för underrättelseinhämtning till den reglering i BfV-lagen som beskrivs ovan. BND har rätt att inom sitt eget ansvarsområde använda sådana metoder för underrättelseinhämtning som anges i 8, 8a och 9 § i BfV-lagen och som det föreskrivs om närmare i BND:s eget reglemente. MAD har en likartad rättighet inom sitt ansvarsområde, även om den inte är lika omfattande.

Enligt 10 § i den tyska grundlagen är skyddet för förtroliga meddelanden okränkbart och inskränkningar i detta får endast föreskrivas genom lag. På grund av detta har regleringen av

metoder för underrättelseinhämtning som är riktade mot innehållet i förtroliga meddelanden samlats i en egen speciallag, G10-lagen, och i den får alla tjänster sina befogenheter.

I G10-lagen föreskrivs det om förutsättningarna för att säkerhets- och underrättelsetjänsterna ska få granska förtroliga meddelanden som förmedlas av posten samt avlyssna och spela in konfidentiell telekommunikation. Utövandet av dessa befogenheter kräver skriftligt tillstånd av det ministerium som ansvarar för verksamheten och ett skriftligt förhandsgodkännande av laglighetsövervakningsorganet (den så kallade G10-kommissionen). Säkerhetstjänsterna inom landet får granska postförsändelser och utföra teleavlyssning endast om det finns skäl att anta att en person planerar att begå en viss typ av brott eller har begått ett sådant brott. I lagen finns en mycket omfattande förteckning över brott som ger befogenhet att inhämta information. Gemensamt för dessa brott är att de kan anses vara riktade mot den nationella säkerheten. Säkerhetstjänsterna inom landet får utöva sina befogenheter också om det med fog kan antas att en person är medlem i en sammanslutning som har för avsikt att begå brott mot den nationella säkerheten. Föremål för utövandet av befogenheterna kan förutom den förmodade gärningsmannen också vara en person som det finns skäl att anta att står i kommunikationsförbindelse med denne. Befogenheterna får endast utövas om det är omöjligt eller väsentligt svårare att inhämta informationen med hjälp av andra metoder. Genom öppnande av postförsändelser eller teleavlyssning får information inte inhämtas om sådana omständigheter som en person får vägra att vittna om med stöd av lagen om straffprocess. Även det så kallade privatlivets kärnområde åtnjuter extra skydd mot myndigheternas informationsinhämtning. Om det finns skäl att anta att en åtgärd endast kommer att frambringa information om privatlivets kärnområde får denna åtgärd inte vidtas. Privatlivets kärnområde utgörs av en persons intima privatliv. Till exempel hör en persons familjeliv inte i sig till privatlivets kärnområde.

Underrättelsetjänsten som avser utländska förhållanden BND får öppna postförsändelser och utföra teleavlyssning, förutom för att upptäcka vissa brott och brottsplaner mot den nationella säkerheten, även när det är nödvändigt för skötseln av de uppgifter som underrättelsetjänsten ålagts i BND-lagen eller för att inhämta information om hot mot liv eller hälsa i fråga om en person som befinner sig i utlandet.

G10-lagens 5 § gäller så kallade strategiska inskränkningar av kommunikationshemligheten (strategische Beschränkungen), det vill säga underrättelseinhämtning som avser datatrafik. Enligt bestämmelsen får underrättelsetjänsten som avser utländska förhållanden BND med tillstånd av det parlamentariska kontrollutskottet, som finns i anslutning till förbundskanslersämbetet och förbundsdagen, utföra underrättelseinhämtning som avser datatrafik, om detta är nödvändigt för att upptäcka och förebygga vissa hot i god tid innan de verkställs. Hot som berättigar till användningen av underrättelseinhämtning som avser datatrafik utgörs bland annat av en beväpnad attack mot Tyskland, internationell terrorism, internationell spridning av krigs- och massförstörelsevapen, yrkesmässig import av narkotika, pengaförfalskning i utlandet som hotar stabiliteten i eurozonen, omfattande organiserad människosmuggling och hot mot liv eller hälsa i fråga om en person som befinner sig i utlandet. Underrättelseinhämtningen som avser datatrafik är baserad på automatiska sökbegrepp och de kan gälla antingen kommunikationsinnehållet eller kommunikationens identifieringsuppgifter. Högst 20 procent av Tysklands internationella datatrafik får övervakas samtidigt genom gallring baserad på sökbegrepp. Sökbegreppen ska anges både i BND:s skriftliga ansökan om tillstånd och i det skriftliga tillståndet av förbundskanslersämbetet och kontrollutskottet, vilket är i kraft i högst tre månader. Sökbegreppen får inte specificera enskilda teleanslutningar och de får inte gälla privatlivets kärnområde. Information om privatlivets kärnområde som eventuellt kommer fram i samband med underrättelseinhämtning som avser datatrafik ska utplånas. Alla uppgifter som inhämtats genom underrättelseinhämtning som avser datatrafik ska bedömas var sjätte månad med avseende på nödvändigheten. Om uppgifterna inte är nödvändiga med tanke på insamlingssyftet och det inte är motiverat att lämna ut dem till någon annan myndighet, ska de ut-

plånas. Uppgifterna får lämnas ut till säkerhetstjänsterna inom landet om det finns konkret anledning att anta att de är nödvändiga för skötseln av tjänsternas lagstadgade uppgifter. Dessutom får uppgifter under vissa förutsättningar lämnas ut till myndigheten för exportkontroll. Utlämnande av uppgifter till polis- och åklagarmyndigheterna och till utländska myndigheter behandlas senare under särskilda rubriker.

Den som är föremål för teleavlyssning och underrättelseinhämtning som avser datatrafik ska underrättas om dessa åtgärder när användningen av metoden för informationsinhämtning har avslutats. Säkerhets- och underrättelsetjänsterna kan dock skjuta upp denna underrättelse om det skulle äventyra syftet med informationsinhämtningen eller det bedöms att det kan vara till skada för förbundsstatens eller en delstats allmänna intressen. Om underrättelsen inte skett inom 12 månader från det att metoden för informationsinhämtning slutade användas, ska förutsättningarna för underrättelsen föras till laglighetsövervakningsmyndigheten (G10-kommissionen) för bedömning. Kommissionen beslutar därefter om hur länge underrättelsen får skjutas upp. Om underrättelsen inte skett inom fem år från det att metoden för informationsinhämtning slutade användas och grunderna för att underrättelsen inte skett kvarstår och med stor sannolikhet kommer att kvarstå även i framtiden, kan G10-kommissionen enhälligt besluta att underrättelsen får utebli.

Rapportering

Varje säkerhets- och underrättelsetjänst rapporterar om sin verksamhet till det styrande ministeriet. Närmare bestämmelser om hur rapporteringsplikten ska uppfyllas finns i säkerhets- och underrättelsetjänsternas sekretessbelagda reglementen. I fråga om rapporteringen är det dock skäl att observera att såväl de styrande ministerierna som det parlamentariska kontrollorganet och laglighetsövervakningsorganet är delaktiga i beslutsfattandet kring användningen av hemliga underrättelseinhämtningsmetoder. På detta sätt får de också förhandsinformation om vissa enskilda operationer som säkerhets- och underrättelsetjänsterna genomför.

Samarbete med brottsbekämpande myndigheter

I vissa av lagarna om underrättelse- och säkerhetstjänsternas verksamhet konstateras det uttryckligen att tjänsterna inte har polisbefogenheter och att de inte har rätt att be polisen utföra sådana åtgärder för dem som de själva inte har rätt att utföra. Däremot föreskrivs det detaljerat om informationsflödet mellan säkerhets- och underrättelsetjänsterna och brottsbekämpningsmyndigheterna.

Säkerhets- och underrättelsetjänsternas skyldighet att meddela om brott till åklagar- och polismyndigheterna anges i 20 § i BfV-lagen och det finns också direkta hänvisningar till denna bestämmelse i lagarna om verksamheten för den militära underrättelsetjänsten MAD och underrättelsetjänsten som avser utländska förhållanden BND. Enligt bestämmelsen ska säkerhets- och underrättelsetjänsterna på eget initiativ till åklagaren och polismyndigheterna lämna ut alla sådana uppgifter som med fog kan antas behövas för förhindrande och utredande av och åtal för brott mot staten. Brott mot staten utgörs inte enbart av brott som anges separat i vissa lagar, utan också av alla sådana straffbara gärningar som kan antas vara riktade mot förbundsstatens eller delstaternas grundlagsenliga samhällsordning, existens eller säkerhet eller Tysklands yttre säkerhet. Anmälningsskyldigheten gäller således sådana brott som i stor utsträckning kan anses höra samman med säkerhets- och underrättelsetjänsternas egna lagstadgade ansvarsområden. Polismyndigheterna har också rätt att av säkerhets- och underrättelsetjänsterna begära och få uppgifter som behövs för att förhindra sådana brott. Säkerhets- och underrättelsetjänsterna behöver dock inte på eget initiativ eller ens på begäran lämna ut uppgifter som behövs för förhindrande eller utredande av brott eller åtal, om till exempel avsevärda säkerhetsintressen motiverar att de inte lämnas ut.

Skyldigheten att lämna ut uppgifter är inte ensidig, eftersom åklagar-, polis- och tullmyndigheterna, liksom förbundsstatens myndigheter, rent allmänt är skyldiga att på eget initiativ informera säkerhets- och underrättelsetjänsterna om hot som hör till deras ansvarsområde. Säkerhets- och underrättelsetjänsterna har också rätt att begära och få uppgifter om hot av brottsbekämpningsmyndigheterna och förbundsstatens myndigheter.

Utöver ömsesidigt utlämnande av information kan säkerhetsmyndigheterna och brottsbekämpningsmyndigheterna inrätta gemensamma projektbaserade personregister när den information som registreras i dem hör till båda parternas uppgifter. Projektbaserade personregister kan endast inrättas för en viss tid.

Om utlämnande av uppgifter som inhämtats med hjälp av metoder för underrättelseinhämtning av innehållet i förtroliga meddelanden till brottsbekämpningsmyndigheter föreskrivs det särskilt i G10-lagen. Information som inhämtats med hjälp av teleavlyssning eller underrättelseinhämtning som avser datatrafik får lämnas ut till åklagar- eller polismyndigheten endast för förhindrande eller utredning av eller åtal för sådana brott som anges uttömmande i förteckningar i lagen. Förteckningarna i G10-lagen över de brott som motiverar utlämnande av uppgifter är i sig mycket omfattande. Den förteckning över brottsbenämningar som finns i anslutning till bestämmelsen om underrättelseinhämtning som avser datatrafik är i viss mån knappare än den förteckning som finns i anslutning till bestämmelsen om teleavlyssning. Brotten i båda förteckningarna kan anses vara riktade mot den nationella säkerheten.

Internationellt samarbete

I lagarna om säkerhets- och underrättelsetjänsternas verksamhet finns inga allmänna bestämmelser om internationellt samarbete. Däremot föreskrivs det i lagarna om de förutsättningar under vilka tjänsterna kan lämna ut personuppgifter till utländska samarbetsmyndigheter.

Enligt 19 § i BfV-lagen och de bestämmelser i MAD- och BND-lagarna som hänvisar till den får säkerhets- och underrättelsetjänsterna lämna ut personuppgifter till utländska myndigheter eller internationella organisationer om det är nödvändigt för att den som lämnar ut uppgifterna ska kunna uppfylla sina lagstadgade uppgifter eller för att skydda mottagarens betydande säkerhetsintressen. Uppgifterna får dock inte lämnas ut om det strider mot Tysklands utrikespolitiska intressen eller övervägande intressen hos den person som är föremål för utlämnandet av information. Utlämnandet ska dokumenteras och mottagaren ska meddelas om att uppgifterna endast får användas i det syfte för vilket de lämnades ut.

Ny lagstiftning om signalspaning som avser utländska förhållanden

BND:s signalspaningsbefogenheter som avser utländska förhållanden kodifieras för första gången i en lag (Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes) som trädde i kraft vid ingången av 2017.

I den nya lagen ställs kravet att signalspaning som avser utländska förhållanden ska vara nödvändig för att i ett tidigt skede upptäcka hot mot förbundsstatens inre eller yttre säkerhet, för att skydda förbundsrepublikens funktionsförmåga eller för att inhämta information som ministerierna i fråga klassificerar som betydelsefulla för utrikes- och säkerhetspolitiken. Signalspaningen som avser utländska förhållanden ska vara baserad på användningen av sökbegrepp. Sökbegreppen kan beskriva såväl personer och organisationer som ämnen. Lagen tillåter under vissa särskilda förutsättningar att underrättelseinhämtning riktas mot Europeiska unionens organ eller unionens medlemsstater. Underrättelseinhämtningen får inte kränka privatlivets kärnområde. Med privatlivets kärnområde avses inte en persons familjeliv eller sociala relationer, utan sådant som hör till intimitetens kärna, såsom sexuellt beteende. I lagen finns också

ett uttryckligt förbud mot ekonomisk underrättelseverksamhet för att främja det tyska näringslivets intressen (Wirtschaftsspionage), men däremot är det tillåtet att inhämta information av finanspolitisk betydelse.

Till skillnad från tidigare är det inte underrättelsetjänsten själv som fattar beslut om användningen av signalspaning som avser utländska förhållanden, utan detta gör förbundskanslersämbetet. Dessutom ska beslutet om användningen av signalspaning som avser utländska förhållanden på förhand godkännas av ett oberoende kontrollorgan (Unabhängiges Kontrollgremium) som inrättades i och med lagen. Det oberoende kontrollorganet består av en ordförande och två ledamöter. Ordföranden och en av ledamöterna ska vara domare i Förbundsrepubliken Tysklands högsta domstol (Bundesgerichtshof) och en ledamot ska vara åklagare i högsta domstolen. Utöver att godkänna beslut om signalspaning utövar organet också tillsyn över verksamheten i efterhand bland annat i form av laglighetsgranskningar. Det undersöker också klagomål som gäller signalspaningen som avser utländska förhållanden. Det oberoende kontrollorganet informerar förbundsdagens kontrollutskott om sin verksamhet med intervaller på högst sex månader.

I lagen finns bestämmelser om internationellt samarbete som utförs inom ramen för signalspaningen som avser utländska förhållanden. BND har tillåtelse att samarbeta med utländska underrättelsemyndigheter om det är nödvändigt för att uppnå syftet med signalspaningen som avser utländska förhållanden och det inte är möjligt att inhämta information på annat sätt. Detaljerna kring samarbetet ska antecknas i ett samförståndsavtal som upprättas mellan parterna. Samförståndsavtalet kan endast gälla informationsinhämtning om internationell terrorism, spridning av massförstörelse- och krigsvapen, utveckling av kriser i utlandet, sådana politiska, ekonomiska eller militära förhållanden i utlandet som kan vara av betydelse för den tyska utrikes- eller säkerhetspolitiken eller andra fall som är jämförbara med dem som nämnts ovan. Dessutom kan samförståndsavtalet gälla signalspaning som behövs för att stödja den tyska försvarsmakten eller allierade stater eller för att bedöma säkerhetsläget för tyska medborgare och allierade staters medborgare i utlandet.

2.4 Förpliktelser som gäller mänskliga rättigheter i internationella konventioner

Allmänt

När det gäller sådana befogenheter som utövas i hemlighet för dem som är föremål för befogenheterna ställs fokus på de grundläggande fri- och rättigheterna och de mänskliga rättigheterna, eftersom sådana befogenheter ofta ingriper i fundamentala rättigheter, till och med i deras kärnområde. Civil underrättelseverksamhet ingriper särskilt i skyddet för privatlivet och skyddet för förtroliga meddelanden samt rättsskyddet.

I detta avsnitt behandlas de väsentliga bestämmelserna i FN:s internationella konvention om medborgerliga och politiska rättigheter och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och den avgörandepraxis som förtydligar dem. I avsnittet behandlas sådana avgöranden som särskilt gäller skyddet för privatlivet och hemligheten i fråga om förtroliga meddelanden.

MP-konventionen

Den internationella konventionen om medborgerliga och politiska rättigheter (MP-konventionen, FördrS 8/1976) godkändes i FN:s generalförsamling 1966 och trädde i kraft i Finland 1976.

Med tanke på integritetsskyddet och skyddet för konfidentiell kommunikation är artikel 17 i konventionen central. Enligt den får ingen utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens, inte heller för olagliga angrepp på sin heder och sitt anseende. Vidare har var och en rätt till lagens skydd mot sådana ingripanden och angrepp. Man får avvika från skyldigheten i artikeln endast vid ett allmänt nödläge som hotar nationens fortbestånd och som officiellt kungjorts som sådant.

Förbudet i artikel 17 mot ingripande i privatlivet och korrespondensen är inte absolut, utan förbudet gäller ”godtyckliga” och ”olagliga” ingripanden i rättigheterna. Konventionsstaterna kan i sin nationella lagstiftning föreskriva om sådana situationer som berättigar till ingripande och om de metoder som ska användas vid ett ingripande. Alla konventionsstater har föreskrivit om ingripande i rättigheterna i brottsbekämpande syfte och många även om ingripande i rättigheterna i syfte att upprätthålla den nationella säkerheten.

Verkställandet av MP-konventionen övervakas av FN:s människorättskommitté som kontinuerligt utvecklar tolkningen av bestämmelserna i konventionen. I människorättskommitténs allmänna kommentar nr 16 från år 1988 (A/43/20) tolkas innehållet i artikel 17 bland annat med tanke på elektronisk kommunikation. Enligt kommentaren är det inte tillräckligt att det i lag har föreskrivits om ingripande i skyddet för privatlivet. Den lagstiftning som berättigar till ingripande får inte vara godtycklig till sitt innehåll och tillämpningen av den får inte heller vara godtycklig. Lagstiftningen måste stå i överensstämmelse med bestämmelserna i och målen med MP-konventionen och i den ska de förhållanden där det är tillåtet att ingripa specificeras noggrant. Ett beslut om en åtgärd som ingriper i integritetsskyddet ska kunna fattas endast för ett specifikt fall och på åtgärd av en myndighet som fastslås i lag och den information som samlas med hjälp av ingripandet ska vara nödvändig med tanke på samhällets intressen (”essential in the interests of society”). Information som anknyter till en persons privatliv får inte användas i syften som står i strid med MP-konventionen.

Flera besvär om kränkning av artikel 17 som gäller integritetsskyddet har anförts med stöd av MP-konventionens fakultativa protokoll, men kommittén har hittills inte behandlat frågor med anknytning till datanätssäkerheten och elektronisk kommunikation. Det kan anses sannolikt att frågor med anknytning till den elektroniska kommunikationens konfidentialitet kommer att bli mera synliga i människorättskommitténs arbete.

Europakonventionen

Skydd för privatlivet

Allmänt

När man bedömer om det ska tillåtas att en lag stiftas om metoder för ingripande i skyddet för privatlivet och skyddet för förtroliga meddelanden är Europakonventionen (FördrS 63/1999), som ingicks inom Europarådet 1950, och till vilken Finland anslöt sig 1989 av större praktisk betydelse än MP-konventionen. Att Europakonventionen följs övervakas av Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen), som i detta syfte behandlar och avgör besvär som gäller konventionsbrott. Europadomstolen har i många av sina avgöranden tagit ställning till hur rätten till skydd för förtroliga meddelanden enligt Europakonventionen bör tolkas. Flera av dessa avgöranden gäller elektronisk kommunikation och några gäller underrättelseinhämtning som avser datatrafik eller former av myndighetsverksamhet som är nära jämförbara med denna.

Enligt artikel 8.1 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Enligt artikel 8.2 i Europakonventionen är rätten

dock inte obegränsad, eftersom myndigheterna får ingripa i denna rättighet med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Enligt etablerad avgörandepraxis i Europadomstolen inbegriper begreppen privatliv och korrespondens, som nämns i artikel 8.1 i Europakonventionen, både telefonkommunikation, e-postkommunikation och annan elektronisk kommunikation som ska anses konfidentiell (bl.a. Klass m.fl. mot Tyskland, 6.9.1978, Kopp mot Schweiz, 25.3.1998, Copland mot Förenade kungariket, 3.4.2007, Liberty m.fl. mot Förenade kungariket, 1.7.2008). Skyddet omfattar både kommunikationens innehåll och kommunikationens identifieringsuppgifter (bl.a. Malone mot Förenade kungariket, 2.8.1984, Weber och Saravia mot Tyskland, 29.6.2006, P.G. och J.H. mot Förenade kungariket, 25.9.2001). I fråga om identifieringsuppgifterna har domstolen särskilt konstaterat att uppgifter till exempel om de telefonnummer som en person har kommunicerat till utgör en organisk del av kommunikationen. Utlämnandet av sådana uppgifter till en myndighet utan samtycke av personen i fråga utgör ett ingripande i dennes privatliv (Malone mot Förenade kungariket).

Myndigheten behöver i själva verket inte behandla uppgifterna för att det ska vara fråga om ingripande i privatlivet, utan som ingripande ska anses det att myndigheten samlar in och sparar dem för senare användning (Marper mot Förenade kungariket, 4.12.2008). Enbart det att sådan lagstiftning existerar, som gör det möjligt att hemligt observera kommunikationsförbindelser, ingriper i de rättigheter som artikel 8 i Europakonventionen garanterar kommunikationsparterna och även potentiella parter (Klass mot Tyskland, Liberty m.fl. mot Förenade kungariket). De potentiella föremålen för övervakningen måste då ha rätt till ett effektivt rättsmedel inför den nationella myndigheten, vilket garanteras i artikel 13 i Europakonventionen. Enligt artikeln ska var och en, vars i denna konvention angivna fri- och rättigheter kränkts, ha tillgång till ett effektivt rättsmedel inför en nationell myndighet och detta även om kränkningen förövats av en person som har handlat i egenskap av offentlig myndighet.

Av detta följer att en person, för att få sitt påstående om att rättigheterna enligt artikel 8 har blivit kränkta prövat av Europadomstolen, inte nödvändigtvis konkret måste visa att myndigheterna har ingripit i hans eller hennes privatliv eller kommunikation. Det räcker med att han eller hon tillhör en sådan människogrupp som rimligtvis kan antas bli föremål för hemliga övervakningsåtgärder på basis av bestämmelser i nationell lag. Om den nationella lagstiftningen till sin karaktär är sådan att det är möjligt att vem som helst blir föremål för kommunikationsobservation, krävs inte ens att personen hör till en sådan människogrupp. Även om sannolikheten för hemlig observation av en person är liten, måste han eller hon i Europadomstolen kunna låta pröva sitt påstående om att rättigheterna enligt artikel 8 i Europakonventionen har blivit kränkta, om effektiva nationella rättsmedel saknas (Klass mot Tyskland, Kennedy mot Förenade kungariket, 18.5.2010, Zakharov mot Ryssland, 4.12.2015, Szabo & Vissy mot Ungern, 12.1.2016). På möjligheterna att få rättsskydd genom Europadomstolen inverkar således såväl ändringssökandens bakgrund och den nationella lagstiftningens karaktär som tillräckligheten i de nationella rättsmedlen.

Tillåtet ingripande i rättigheter enligt artikel 8.1 i Europakonventionen

Att kommunikationens innehåll och identifieringsuppgifter omfattas av skydd enligt artikel 8 i Europakonventionen betyder inte att myndigheterna inte kan ingripa i dem. Ingripandet i privatlivet kan till och med vara jämförelsevis omfattande när det sker inom ramen för artikel 8.2 i Europakonventionen. I artikel 8.2 ställs tre villkor för att man i myndighetsverksamhet ska kunna ingripa i de rättigheter som artikeln garanterar: 1) ingripandet ska tillåtas i nationell lag, 2) det ska göras för att trygga vissa intressen som särskilt räknas upp i artikeln och 3) det ska

vara nödvändigt i ett demokratiskt samhälle. Den nationella säkerheten är ett av de intressen som gör det möjligt att ingripa i skyddet för privatlivet och därmed också i skyddet för konfidentiell kommunikation.

Kravet på att ingripandet ska grunda sig på lag

Ingripande i de rättigheter som garanteras i artikel 8 i Europakonventionen ska grunda sig på nationell lag. Betydelsen av detta krav framträder i synnerhet då man ingriper i rättigheter i hemlighet för den som är föremål för ingripandet. Gränserna för en myndighets prövningsrätt och sätten att använda prövningsrätten ska fastställas tillräckligt tydligt i lag för att möjligheten till godtycklighet vid hemligt användande av verkställande makt ska kunna avvärjas (Malone mot Förenade kungariket, Amann mot Schweiz, 16.2.2000, Telegraaf Media Nederland Landelijke Media B.V. m.fl. mot Nederländerna, 22.11.2012, Rotaru mot Rumänien, 4.5.2000).

I sina avgöranden har Europadomstolen upprepade gånger betonat att en lag som möjliggör att hemliga myndighetsåtgärder ingriper i skyddet för privatlivet måste vara förenlig med rättsstatsprinciperna, tillgänglig för medborgarna samt till sin art sådan att medborgarna kan förutse vilka följder tillämpningen av den har för dem själva (bl.a. Kruslin mot Frankrike, Huvig mot Frankrike, 24.4.1990 Lambert m.fl. mot Frankrike, 5.6.2015). Den ska vara tillräckligt tydlig [”sufficiently clear in its terms”] för att ge en adekvat indikation [”an adequate indication”] om under vilka omständigheter och förutsättningar medborgarna kan bli föremål för hemliga myndighetsåtgärder (Kopp mot Tyskland, Kruslin mot Frankrike, 24.4.1990, Huvig mot Frankrike). Lagen får inte vara sådan att den möjliggör att hemlig observation riktas slumpmässigt mot vem som helst (Amann mot Schweiz). Att det i lagen till exempel enbart nämns att hemliga befogenheter får användas för att skydda den nationella säkerheten, är inte tillräckligt för att uppfylla kravet på förutsebarhet (Zakharov mot Ryssland). Man kan inte heller kräva att den nationella lagstiftningen på ett exakt och uttömmande sätt ska ange alla de situationer där myndigheterna får använda hemliga befogenheter. En bestämmelse i lagen om att terrorhot är en grund för utövande av hemliga befogenheter kan till exempel anses uppfylla kravet på förutsebarhet som ställs i Europakonventionen (Szabo & Vissy mot Ungern).

Vid bedömningen av om kravet på förutsebarhet uppfylls ska också förordningar och myndighetsföreskrifter beaktas vid sidan av den egentliga lagen som stiftas av parlamentet. De bestämmelser på mycket allmän nivå som finns i den egentliga lagen kan preciseras med hjälp av instrument på lägre nivå. Dessa ska dock vara offentliggjorda – sådana interna myndighetsföreskrifter som inte är tillgängliga för medborgarna uppfyller inte kravet på förutsebarhet (t.ex. Silver m.fl. mot Förenade kungariket, 25.3.1983, Malone mot Förenade kungariket). I en lag som är allmänt tillgänglig ska åtminstone karaktären på och omfattningen av de observationsbefogenheter som utövas i hemlighet, de personkategorier som riskerar att bli föremål för befogenheterna, karaktären av sådan verksamhet som motiverar användningen av befogenheterna, de förfaranden som används när de uppgifter som inhämtats med hjälp av befogenheterna undersöks, används, lagras, lämnas ut eller raderas, bestämmelser om övervakningen av befogenheterna och de rättsmedel som gäller dem definieras (Amann mot Schweiz, Valenzuela Contreras mot Spanien, 30.7.1998, Prado Bugallo mot Spanien, 18.2.2003 Shimovolos mot Ryssland). Kraven på förutsebarhet i lagstiftningen ska ställas oberoende av om det är fråga om observation av enskilda personers kommunikationsförbindelser på grund av brottsmisstankar eller storskalig allmän övervakning av kommunikationsförbindelser på grund av misstankar om hot (Weber och Saravia mot Tyskland, Liberty m.fl. mot Förenade kungariket).

Europadomstolen har i fyra viktiga avgöranden som den träffat under de senaste åren bedömt om underrättelseinhämtning som avser datatrafik och förfaranden som är nära jämförbara med den är förenliga med Europakonventionen. I fallet Liberty m.fl. mot Förenade kungariket an-

såg den att den nationella lagstiftning som möjliggjorde underrättelseinhämtning som avser datatrafik till sin art var sådan att den inte uppfyllde kravet i artikel 8.2 i Europakonventionen om att hemlig observation ska ske med stöd av lag. I fallet Weber och Saravia mot Tyskland kom domstolen till motsatt resultat – den nationella lagstiftningen uppfyllde de krav som ställs på lagens kvalitet och var därmed förenlig med Europakonventionen. I avgörandet Zakharov mot Ryssland i slutet av 2015 ansåg domstolen att den ryska lagstiftningen stod i strid med Europakonventionen för att den inte uppfyllde kvalitetskraven i artikel 8, då sådant ingripande som möjliggjordes i lagstiftningen inte var nödvändigt i ett demokratiskt samhälle på det sätt som avses i artikeln. I avgörandet Szabo & Vissy mot Ungern från början av 2016 konstaterade domstolen att den ungerska lagen stred mot Europakonventionen framför allt för att den bröt mot kravet på att ett ingripande ska vara nödvändigt i ett demokratiskt samhälle. För att underlätta läsbarheten behandlas alla dessa fyra centrala avgöranden om underrättelseinhämtning som avser datatrafik i sin helhet under denna rubrik. Några av de synpunkter som framkommer presenteras senare då kravet på att ett ingripande ska vara nödvändigt i ett demokratiskt samhälle i artikel 8 i Europakonventionen behandlas.

I fallet Liberty m.fl. mot Förenade kungariket var det frågan om en storskalig övervakning av telefontrafiken till utlandet som Storbritanniens signalspaningsverk, som lyder under försvarsministeriet, hade utfört. Inom ramen för denna övervakning kunde man samtidigt avlyssna till och med 10 000 telefonlinjer. I sig var frågan obestridlig, eftersom verksamheten grundade sig på en nationell lag. Enligt denna lag kunde inrikesministern ge olika säkerhetsmyndigheter tillstånd [”warrant”] att rikta informationsinhämtning mot kommunikationsförbindelser mellan Storbritannien och utlandet. I tillstånden definierades de kommunikationsförbindelser som informationsinhämtningen kunde riktas mot på en mycket allmän nivå (t.ex. ”alla meddelanden som förmedlas i sjökablar mellan Storbritannien och det övriga Europa”). I samband med att tillstånd beviljades skulle inrikesministern definiera det material som informationsinhämtningen skulle gälla. Enligt lagen räckte det emellertid som definition att den information som skulle inhämtas enligt inrikesministerns uppfattning behövdes antingen för att upprätthålla den nationella säkerheten, förebygga eller avslöja allvarlig brottslighet eller för att trygga landets ekonomiska intressen. När tillstånd beviljades skulle inrikesministern också meddela sådana hemliga föreläggande som han eller hon ansåg nödvändiga för att säkerställa att sådana meddelanden som inte omfattades av tillståndet inte skulle bli granskade och att de meddelanden som skulle granskas avslöjades eller kopierades endast i behövlig omfattning. I lagen fanns inga närmare bestämmelser om dessa föreläggandens innehåll eller område. Efter att ha fått tillstånd av inrikesministern skapade säkerhetsmyndigheterna självständigt de automatiska sökbegrepp med hjälp av vilka den information som gällde den nationella säkerheten eller andra i lagen nämnda intressen filtrerades ur all kommunikation. Säkerhetsmyndigheterna hade sina egna interna bestämmelser om på vilka grunder de uppgifter som var resultatet av filtreringen behandlades, sparades, delades och raderades, men dessa bestämmelser var inte offentliga eller allmänt tillgängliga.

I sitt avgörande i ärendet konstaterade Europadomstolen att enligt lagen kunde inrikesministerns tillståndsbeslut omfatta vilket meddelande som helst, vilket gjorde att vilket som helst meddelande som vem som helst skickade till utlandet eller fick därifrån kunde fångas upp. Följaktligen hade den verkställande makten i fråga om att fånga upp utländska meddelanden beviljats en i praktiken obegränsad prövningsrätt. Lagen tillät också en bred prövningsmarginal i fråga om vilka meddelanden som faktiskt granskades. I detta hänseende var det tillräckligt att inrikesministern ansåg granskningen nödvändig med tanke på den nationella säkerheten eller andra i lagen nämnda och allmänt formulerade intressen. I lagen fanns inga närmare bestämmelser om behandlingen av meddelanden som inte omfattades av tillståndet och de föreläggande som inrikesministern utfärdat i saken var inte offentliga. I sammandrag konstaterade Europadomstolen att gränserna för den mycket vida prövningsrätten som beviljats för uppfångandet och granskandet av meddelanden inte genom den nationella lagen hade anvisats

tillräckligt klart för den verkställande makten. I synnerhet hade det inte angetts offentligt hur gallringen, användningen, förvaringen och utplåningen av uppfångat material skulle genomföras. Således uppfyllde Storbritanniens signalspaningslagstiftning inte de kvalitetskrav som ställs i artikel 8.2 i Europakonventionen och ett brott mot Europakonventionen hade begåtts.

I fallet Weber och Saravia mot Tyskland var det frågan om storskalig så kallad strategisk övervakning som Tysklands underrättelsetjänst BND hade bedrivit i fråga om mobiltelefontrafiken mellan Tyskland och utlandet och som det föreskrevs om i nationell lag. Enligt denna lag fick strategisk övervakning av mobiltelefontrafiken bedrivas för att avvärja vissa särskilt angivna hot som riktade sig mot den nationella säkerheten. Sådana i lagen angivna hot var en militärattack mot Tyskland, terrordåd som skulle genomföras i Tyskland och till sin art var internationella, internationell smuggling av vapen, storskalig import av droger, penningförfalskning utomlands och penningtvätt med anknytning till ovannämnda fenomen. En minister i förbundsstaten beviljade tillstånd för varje enskild strategisk övervakningsuppgift efter att först ha hört det parlamentariska kontrollorganet med anledning av tillståndsansökan. De automatiska sökbegrepp med hjälp av vilka avsikten var att filtrera mobiltelefontrafiken skulle framgå både av BND:s tillståndsansökan och av det tillstånd som ministern beviljade. I lagen fanns bestämmelser om hur det material som hade filtrerats skulle behandlas och i vilka fall personuppgifter, som dykt upp genom filtreringen, fick användas för att förhindra, avslöja och utreda brott. I lagen fanns också bestämmelser om när den filtrerade informationen skulle anses vara irrelevant och hur man skulle hantera sådan information. Vidare föreskrevs det i lagen om giltighetstiderna för övervakningstillstånden, om hur länge filtrerade uppgifter skulle bevaras, om utplåning av uppgifter samt om grunder och förutsättningar för att uppgifterna skulle kunna lämnas ut till andra myndigheter.

Europadomstolen ansåg att den tyska lagstiftningen uppfyllde de krav på kvalitet och förutsebarhet som ställdes på lagen med stöd av artikel 8.2 i Europakonventionen. Viktigt i detta hänseende var bland annat att de hot som skulle avvärjas med hjälp av övervakning angavs i lagen. Lagen ansågs också erbjuda en tillräcklig anvisning om vilka personkategorier övervakningen enligt lagen kunde riktas mot. De automatiska sökbegrepp som användes för att inrikta övervakningen skulle direkt med stöd av lagen framgå av de tillstånd som beviljades för övervakningen och då hade den myndighet som bedrev övervakningen inte obegränsad prövningsrätt för att definiera dem. Med tanke på att kravet på förutsebarhet skulle uppfyllas var det också av betydelse att det i lagen angavs maximitider för tillståndens giltighet och bestämmelser om de förfaranden som skulle följas när uppgifterna granskades och utnyttjades. Likaså var det enligt Europadomstolen av betydelse att det i lagen föreskrevs om de begränsningar och villkor som skulle följas då uppgifter lämnades vidare samt om de förhållanden under vilka uppgifterna skulle utplånas. I sitt avgörande i fallet Weber och Saravia konstaterade Europadomstolen även särskilt att den allmänna övervakningen av kommunikationsförbindelser som bedrivs på tyskt territorium i princip inte kan kränka andra länders statssuveränitet fastän den ena parten i kommunikationen skulle befinna sig i ett sådant annat land.

Det nya avgörandet Zakharov mot Ryssland är anmärkningsvärt, eftersom Europadomstolen i detta fall inte enbart tog ställning till det formella innehållet i den ryska lagen, utan även i hög grad till den praktiska tillämpningen av den. Avgörandet gällde den övervakning av post-, tele- och kommunikationstrafiken som den ryska interna säkerhetstjänsten FSB bedrev för egen del och på uppdrag av andra myndigheter och som det föreskrevs om i nationell lag. Enligt lagen var det i Ryssland tillåtet att ingripa i skyddet för förtroliga meddelanden, som är en grundläggande rättighet, för att 1) förhindra, avslöja och undersöka brott av en viss allvarlighetsgrad samt identifiera personer som begår eller som har begått sådana brott, 2) spåra efterlysta personer samt försvunna personer och 3) skaffa fram information om händelser eller verksamhet som hotar Rysslands nationella, militära, ekonomiska eller ekologiska säkerhet. Beslutet om ingripande i konfidentiell kommunikation fattades av en domstol och i nationell

lag fanns bestämmelser om hur den inhämtade informationen skulle sparas, användas, utplånas och utlämnas samt hur den person som var föremål för informationsinhämtningen skulle underrättas om detta.

Domstolen ansåg att den ryska lagstiftningen stred mot artikel 8 i Europakonventionen framför allt på följande grunder:

- I den nationella lagen varken preciserades eller beskrevs hurdana händelser eller hurdan verksamhet som skulle anses kunna äventyra Rysslands nationella, militära, ekonomiska eller ekologiska säkerhet, varför lagen inte uppfyllde kravet på förutsebarhet som följer av artikel 8 i Europakonventionen. Den makt som säkerhetsmyndigheterna fått för att pröva hurdana och hur allvarliga händelser eller åtgärder som gav rätt till hemlig övervakning var i det närmaste obegränsad. Fastän det i Ryssland föreskrevs om det rättsliga tillståndsförfarandet och ett sådant förfarande normalt är en viktig garanti mot godtyckighet i myndigheternas verksamhet, var förfarandet i det här fallet inte tillräckligt effektivt på grund av att de kriterier i lagen som styrde domstolens tillståndsprövning var alltför vaga.

- I den nationella lagen fanns inga bestämmelser om i vilka situationer som användningen av hemlig observation skulle avslutas. I lagen angavs den maximala längden för observationsåtgärder till sex månader, vilket domstolen i sig ansåg vara lämpligt. I lagen föreskrevs dock inte att utövandet av befogenheterna skulle avlutas innan tidsfristen löpt ut, om förutsättningarna för utövandet av befogenheterna inte längre var uppfyllda. Regleringen innehöll således inte heller till denna del tillräckliga garantier mot godtyckligt utövande av befogenheterna.

- Enligt den nationella lagen skulle den information som inhämtats genom observationsåtgärder utplånas efter sex månader om åtal inte väckts mot den person som varit föremål för åtgärderna. Domstolen ansåg att de bestämmelser som gällde förvaringstiden i sig var ändamålsenliga, men ansåg att bevarandet av information som var klart oväsentlig stred mot Europakonventionen. Med andra ord förpliktade lagen inte myndigheterna till att omedelbart utplåna information som den konstaterat vara irrelevant.

- Europadomstolen ansåg det vara en viktig principiell rättsskyddsgaranti att en domstol i enlighet med rysk lag fattar beslut om ingripande i skyddet för förtroliga meddelanden efter en motiverad ansökan av en myndighet. I lagen fanns dock inte tillräckliga kriterier som styrde domstolens rättsliga prövning. De hot som kunde ge fog för hemlig observation hade definierats så brett i lagen att beslutsfattandet i själva verket snarare kunde anses utföras av den säkerhetsmyndighet som lämnade in ansökan än den domstol som formellt godkände den. I lagen ställdes inte heller krav på att användningen av den metod för informationsinhämtning som ansökan gällde skulle vara nödvändig (necessary, se diskussionen kring begreppets betydelseinnehåll under rubriken ”Nödvändigheten av ingripande i ett demokratiskt samhälle”) och proportionerlig för att ansökan skulle godkännas. Dessutom konstaterade Europadomstolen att de ryska domstolarna i själva verket vanligen inte förutsatte att ansökningarna motiverades eller att skriftligt material som understödde dem lades fram, utan för att ansökningarna skulle godkännas räckte det i praktiken med att säkerhetsmyndigheten framförde ett ospecificerat påstående om att den nationella, militära, ekonomiska eller ekologiska säkerheten var hotad.

- Europadomstolen hänvisade till sin tidigare avgörandepraxis (bl.a. Klass mot Tyskland, Liberty m.fl. mot Förenade kungariket och Kennedy mot Förenade kungariket) enligt vilken det av beslutet om informationsinhämtningsmetoden för ingripande i skyddet för förtroliga meddelanden tydligt ska framgå vem som är föremål för åtgärden eller någon annan specificerande faktor (”a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorization is ordered”). Som exempel på sådana specifice-

rande faktorer nämnde domstolen namn, adresser, telefonnummer eller ”annan relevant information”. (Enligt avgörandet Weber & Saravia mot Tyskland kan sådan ”annan relevant information” betyda tillräckligt specificerade sökbegrepp.) I rysk lag fastställdes inga kriterier för hur åtgärder som ingriper i skyddet för förtroliga meddelanden skulle riktas mot en person eller på något annat sätt. Därmed hade domstolarna till exempel beviljat tillstånd som tillät att alla personers telefonanslutningar i ett visst område avlyssnades. I några fall innehöll tillstånden ingen information om giltighetstiden. Således hade myndigheterna en särdeles omfattande prövningsrätt i fråga om vilka personers telefonanslutningar som avlyssnades och hur länge detta kunde pågå.

- I den nationella lagen föreskrevs det om beslutsförfarandet i brådskande situationer att myndigheterna fick avlyssna konfidentiell kommunikation under 48 timmar utan tillstånd av domstol. Myndigheten måste informera domstolen om sitt brådskande beslut inom 24 timmar och om domstolen inte hade beviljat tillståndet inom 48 timmar efter att avlyssningen hade inletts måste den stoppas. Europadomstolen har i sin tidigare avgörandepraxis konstaterat att särskilda bestämmelser om beslutsförfarandet i brådskande situationer kan vara godtagbara, om det av den nationella lagen tydligt framgår att sådant beslutsförfarande kan tillämpas endast i undantagsfall och när det finns nödvändiga skäl för detta (Association for European Integration and Human Rights och Ekimdzhiev mot Bulgarien). Den ryska lagen uppfyllde dock inte de här villkoren, eftersom den inte innehöll några kriterier som begränsade när beslutsförfarandet i brådskande situationer fick användas. På så sätt gav lagen i själva verket myndigheterna fri prövningsrätt att besluta i vilka situationer det var befogat att använda förfarandet. I lagen föreskrevs det inte heller om någon möjlighet för domstolen att i efterhand utvärdera om användningen av förfarandet hade varit befogat eller att den information som samlats in med stöd av ett myndighetsbeslut som saknade grund skulle utplånas.

- Rysslands kommunikationsministerium hade genom en föreskrift ålagt alla leverantörer av kommunikationstjänster att installera sådan utrustning i sina utrymmen att detta gav säkerhetsmyndigheterna direkt tillgång till alla mobiltelefonanslutningar för samtliga användare. Dessutom hade kommunikationsministeriet ålagt tjänsteleverantörerna att skapa databaser för att i tre år lagra information om samtliga abonnenters kommunikationsförbindelser. Enligt ministeriets föreskrift skulle säkerhetsmyndigheterna ha direkt fjärråtkomst till databaserna. Den ryska lagen förpliktade däremot inte säkerhetsmyndigheterna att för tjänsteleverantörerna uppvisa ett domstolstillstånd för hemliga observationsåtgärder innan åtgärden utfördes. Enligt Europadomstolen är ett system som gör det tekniskt möjligt för myndigheterna att fånga upp kommunikation av vilken person som helst direkt, utan hänsyn till om det finns tillstånd för åtgärden eller inte, särskilt mottagligt för missbruk.

- Europadomstolen har i sin tidigare avgörandepraxis (bl.a. Kennedy mot Förenade kungariket) betonat att myndighetsåtgärder som ingriper i skyddet för förtroliga meddelanden noggrant ska dokumenteras för laglighetsövervakningen. Den ryska lagen förutsatte dock ingen dokumentation, utan rent av förbjöd den. I och med att de ryska myndigheterna hade fått direkt anslutning till uppgifter om medborgarnas kommunikationsförbindelser och det inte dokumenterades något om de myndighetsåtgärder som utfördes med hjälp av dessa anslutningar, ledde detta till att laglighetsövervakaren saknade reell möjlighet att få information om myndigheternas lagstridiga åtgärder.

- De domstolar som ansvarade för att bevilja tillstånden hade ingen lagstadgad behörighet att övervaka att tillstånden verkställdes i enlighet med lagen. I den nationella lagen hade i stället åklagarväsendet fått till uppgift att genomföra laglighetsövervakningen. På basis av sin tidigare avgörandepraxis ansåg Europadomstolen att åklagarna inte hade en tillräckligt självständig ställning i Ryssland i förhållande till det som skulle övervakas. Redan i sitt avgörande Iordachi m.fl. mot Moldavien konstaterade Europadomstolen att anvisande av uppgifterna om

laglighetsövervakning till riksåklagarämbetet och det åklagarväsende som lyder under det inte uppfyller kravet på oberoende i laglighetsövervakningen. I fråga om Ryssland konstaterade Europadomstolen att det faktum att åklagarna utsågs och avsattes från sina tjänster av riksåklagaren efter överläggningar med de regionala verkställande myndigheterna var tillräckligt för att ifrågasätta åklagarväsendets oberoende av den verkställande makten. Det att laglighetsövervakningen hörde till åklagarnas uppgifter kunde också ge upphov till situationer med intressekonflikter, eftersom det var åklagarna som i Ryssland beviljade tillstånd för sådana åtgärder som ingriper i skyddet för förtroliga meddelanden som utförs under förundersökningar.

- Utöver att Europadomstolen ifrågasatte laglighetsövervakarens oberoende ansåg den också att åklagarnas lagstadgade befogenheter för laglighetsövervakningen var otillräckliga för att de skulle kunna utöva denna effektivt och kontinuerligt. I den ryska lagen föreskrevs om åklagarnas rätt att inspektera säkerhetsmyndigheternas verksamhet i och med laglighetsövervakningen och inom ramen för detta hade åklagarna tillgång till sekretessbelagt material. Enligt Europadomstolen var tillgången till de sekretessbelagda uppgifterna trots allt begränsad på ett sätt som ifrågasatte laglighetsövervakningens effektivitet, eftersom åklagarna inte hade rätt att bekanta sig med uppgifter om täckoperationer. Laglighetsövervakarnas rätt att bekanta sig med åtgärder som ingrep i skyddet för konfidentiell kommunikation i anslutning till säkerhetstjänstens kontraspionage var begränsad till fall där den som var föremål för åtgärden hade anfört klagan om åtgärden. Eftersom säkerhetsmyndigheterna inte var skyldiga att underrätta den som var föremål för en åtgärd om åtgärden, var möjligheten att anföra klagan obefintlig, vilket i sin tur ledde till att säkerhetstjänstens kontraspionageverksamhet i själva verket stod utanför laglighetsövervakningen.

- Enligt de nationella bestämmelserna hade den åklagare som utförde laglighetsövervakningen rätt att beordra säkerhetsmyndigheterna att avsluta lagstridig informationsinhämtning liksom att vidta åtgärder för att de ansvariga skulle ställas till svars. Europadomstolen konstaterade att bestämmelserna inte var tillräckliga, eftersom det i lagen inte förutsattes att den information som inhämtats på ett lagstridigt sätt skulle utplånas.

- Europadomstolen ansåg att regleringen av laglighetsövervakningen också var bristfällig till de delar som den inte förutsatte tillräckligt transparent rapportering om de iakttagelser som gjorts vid laglighetsövervakningen. Enligt nationell lag skulle åklagarna lämna in rapporter om sina iakttagelser vid inspektionerna halvårsvis till riksåklagarämbetet, men i rapporterna skilde man inte mellan metoder för informationsinhämtning som ingrep i skyddet för förtroliga meddelanden och övrig informationsinhämtning. Dessutom var rapporterna rent statistiska – i dem presenterades antalet informationsinhämtningsåtgärder och antalet upptäckta överträdelser vid inspektionerna, men inga uppgifter om karaktären på dessa överträdelser eller vilka åtgärder som eventuellt hade vidtagits för att gottgöra dessa. Eftersom rapporterna också var sekretessbelagda i sin helhet, var laglighetsövervakningen inte underkastad någon offentlig granskning.

- Europadomstolen konstaterade att den ryska regeringen inte hade framfört ett enda praktiskt exempel på fall där en laglighetsövervakare uppmanat den som var föremål för laglighetsövervakningen att upphöra med eller gottgöra för de lagstridiga åtgärderna. Regeringen hade därmed inte heller i praktiken lyckats visa att övervakningsarrangemangen fungerade och var effektiva.

- Europadomstolen har i flera tidigare avgöranden tagit ställning till om den som är föremål för informationsinhämtning ska ha rätt att och i så fall i vilka situationer få information av myndigheten om de åtgärder för informationsinhämtning som han eller hon har varit föremål för. I fallen Klass mot Tyskland och Weber & Saravia mot Tyskland ansåg Europadomstolen att bestämmelser om att den som varit föremål för informationsinhämtning ska underrättas

genast när detta inte längre äventyrar syftet med informationsinhämtningen var godtagbara med tanke på Europakonventionen. Europadomstolen påpekade också att enligt det tyska systemet svarade ett oberoende organ (G10-kommissionen) och inte säkerhetsmyndigheten för bedömningen av förutsättningarna för att underrätta eller inte underrätta. I fallen Association for European Integration and Human Rights och Ekimdzhiev mot Bulgarien och Dumitru Popescu mot Rumänien konstaterade Europadomstolen att nationell reglering som innebär att den som är föremål för informationsinhämtningen inte alls behöver underrättas vanligen strider mot Europakonventionen. När Europadomstolen nu bedömde den ryska lagstiftningen konstaterade den att lagstiftningen inte förutsatte att den som var föremål för informationsinhämtningen vid något tillfälle skulle underrättas. För en sådan person var det möjligt att få reda på att han eller hon hade varit föremål för informationsinhämtning endast i sådana fall då åtal väcktes mot honom eller henne. När merparten av dem som varit föremål för informationsinhämtning aldrig fick reda på att de hade varit det, kunde de inte heller söka rättsskydd mot lagstridig myndighetsverksamhet. För att den ryska lagen skulle tillåta möjligheten att anföra klagan krävdes att klaganden exakt kunde specificera det beslut som var föremål för klagomålet, vilket naturligtvis inte var möjligt om han eller hon inte alls var medveten om att ett sådant beslut existerade. På grund av detta ansåg Europadomstolen att det i den ryska lagen inte fanns bestämmelser om effektiva rättsmedel, vilket krävs i artikel 13 i Europakonventionen.

Med anledning av de många brister som presenterats ovan bedömde Europadomstolen att den ryska lagstiftningen inte uppfyllde de krav på kvalitet och förutsebarhet som ställs på nationella lagar i artikel 8 i Europakonventionen. Samtidigt konstaterade den att den ryska lagstiftningen inte förmådde avgränsa ingripandet i de mänskliga rättigheterna enligt artikel 8 i Europakonventionen till en nivå som var nödvändig i ett demokratiskt samhälle. Även om fallet Zakharov också var nära sammankopplat med frågan om förekomsten av effektiva nationella rättsmedel i enlighet med artikel 13 i Europakonventionen, tog Europadomstolen i sitt avgörande inte särskilt ställning till påståendet om att artikeln hade kränkts.

I det för tillfället nyaste fallet som gäller underrättelseinhämtning som avser datatrafik, Szabo & Vissy mot Ungern, utförde Ungerns säkerhetstjänst mot terrorism underrättelseinhämtning riktad mot elektronisk kommunikation. Enligt den nationella lagen var en legitim grund för sådan underrättelseinhämtning för det första att förhindra terrordåd och för det andra att rädda ungerska medborgare i nöd i utlandet. Tillstånd för underrättelseinhämtningen beviljades av justitieministern på begäran av säkerhetstjänsten mot terrorism. Säkerhetstjänsten måste i sin ansökan om tillstånd nämna den person eller de grupper av personer i vilkas elektroniska kommunikation det var meningen att ingripandet skulle ske eller åtminstone nämna uppgifter som skulle göra det möjligt att identifiera de här personerna eller grupperna. Ansökan om tillstånd måste dessutom innehålla en redogörelse för den underrättelseinhämtningsuppgift som var grund för informationsinsamlingen samt för nödvändigheten av den.

Europadomstolen konstaterade att det var obestridligt att grunden för ingripandet var att skydda den nationella säkerheten och ansåg vidare att specificeringen på lagnivå av de hot som var föremål för underrättelseverksamheten var tillräcklig för att uppfylla kravet på förutsebarhet i artikel 8. Trots detta ansåg Europadomstolen att Ungerns lagstiftning efter en helhetsbedömning stod i strid med Europakonventionen. Fyra faktorer inverkade på domstolens helhetsbedömning. För det första förutsattes det inte i lagen att säkerhetstjänsten i sin ansökan om tillstånd på något sätt skulle visa att de personer eller grupper av personer som var föremål för ansökan hade ett verkligt eller förmodat samband med det hot som det skulle samlas information om genom underrättelseverksamheten. Även om säkerhetstjänsten i sin ansökan om tillstånd skulle motivera att underrättelseverksamheten var nödvändig, behövde den inte presentera fakta som stöd för sin ansökan. Domstolen konstaterade att ett krav på presentation av fakta skulle göra det möjligt att bedöma om åtgärden för underrättelseinhämtning var nödvän-

dig utifrån individuella misstankar om de personer eller grupper av personer som var föremål för åtgärden. För det andra konstaterade domstolen att bestämmelsen i den nationella lagen om längden för åtgärderna för informationsinhämtning var alltför vag. Utifrån den förblev det oklart om tillståndet för underrättelseinhämtning kunde förnyas endast en gång eller upprepade gånger efter att tillståndets giltighetstid hade löpt ut. För det tredje ansåg domstolen att det lagstadgade tillståndsförfarandet inte var korrekt. Enligt domstolen fanns det inte tillräckliga garantier mot missbruk i fråga om förfarandet, då den som avgjorde om tillstånd skulle beviljas var en representant för den verkställande makten som utsetts till sin tjänst på politiska grunder. För det fjärde konstaterade domstolen att den ungerska lagstiftningen i praktiken inte erbjöd några rättsmedel för dem som eventuellt fått sina rättigheter kränkta. Eftersom det i den ungerska lagstiftningen inte alls förutsattes att de som varit föremål för hemliga övervakningsåtgärder skulle underrättas om detta, hade de här personerna inga möjligheter att ifrågasätta om åtgärderna hade varit lagenliga.

Den nationella säkerheten som ett intresse som berättigar till ingripande

Den nationella säkerheten är ett av de intressen som enligt artikel 8.2 i Europakonventionen kan berättiga till ingripande i skyddet för privatlivet. Europadomstolen har i sin rättspraxis sällan ifrågasatt de svarande staternas invändningar om att ett ingripande har skett på grund av den nationella säkerheten. Det verkar som att staterna har en bred prövningsmarginal för hurdan verksamhet som de anser hota den nationella säkerheten och därmed kan berättiga till ett ingripande i de rättigheter som garanteras i artikel 8 i Europakonventionen. Bakgrunden till detta är att den nationella säkerheten av hävd hör till statssuveräniteten (Bucur och Toma mot Rumänien). Utifrån domstolens avgörandepraxis står det klart att åtminstone militärt försvar, bekämpande av terrorism och avvärjande av olaglig underrättelseverksamhet hör till den nationella säkerheten (bl.a. Klass mot Tyskland, Weber och Saravia mot Tyskland). Många olika typer av hot kan riktas mot den nationella säkerheten och de kan vara svåra att förutse eller definiera på förhand. Av detta följer att begreppet i första hand ska förtydligas genom nationell praxis (Kennedy mot Förenade kungariket). Det att gränsen mellan den nationella säkerheten och andra tillåtna grunder (såsom den allmänna säkerheten och förebyggande av oordning eller brott) att ingripa i de rättigheter som garanteras i artikel 8 i Europakonventionen kan tyckas vackla från fall till fall kan i sig öka staternas prövningsrätt. Av Zakharov-avgörandet framgår det däremot att sådana händelser och situationer som utgör ett hot mot den nationella säkerheten och som därför berättigar till ingripande i de rättigheter som garanteras i artikel 8 med en viss precision måste beskrivas och specificeras i de nationella lagarna. Med andra ord får begreppet nationell säkerhet inte lämnas helt öppet i de nationella lagstiftningarna, eftersom detta inte uppfyller kravet på förutsebarhet i lagstiftningen som ställs i artikel 8 i Europakonventionen. Enligt avgörandet Szabo och Vissy innebär kravet på förutsebarhet dock inte att hotsituationerna måste definieras helt exakt och uttömmande på lagnivå.

Nödvändigheten av ingripande i ett demokratiskt samhälle

Det tredje och sista villkoret för att myndigheterna ska få ingripa i utövandet av de rättigheter som garanteras i artikel 8 i Europakonventionen är att ingripandet ska vara nödvändigt i ett demokratiskt samhälle. Ordet ”nödvändig” som används i den svenskspråkiga versionen av artikeln måste i någon mån anses omöjligt att avgränsa, eftersom Europadomstolen gett följande utlåtande om betydelseinnehållet för den engelskspråkiga motsvarigheten: ”the adjective ”necessary” is not synonymous with ”indispensable”, neither has it the flexibility of such expressions as ”admissible”, ”ordinary”, ”useful”, ”reasonable” or ”desirable” (Handyside mot Förenade kungariket). Detta torde innebära att den nödvändighet som avses i artikeln placerar sig någonstans mellan oumbärlig och behövlig. Härnäst framgår dock att Europadomstolen i sina senaste avgöranden skärpt tolkningen av kravet på nödvändighet speciellt i kontexter som gäller underrättelseinhämtning som avser datatrafik.

Kravet på nödvändighet i ett demokratiskt samhälle innefattar att ingripandet i rättigheterna ska svara mot ett trängande samhällsbehov (correspond to a pressing social need). Av kravet följer också att ingripandet ska ske i enlighet med proportionalitetsprincipen: ingripandet ska stå i förnuftig proportion till det syfte som tillåts enligt artikel 8.2 i Europakonventionen och som åberopas som legitim grund för ingripandet (bl.a. Gillow mot Förenade kungariket, Silver m.fl. mot Förenade kungariket, Handyside mot Förenade kungariket).

I första hand eller åtminstone i det första skedet är det den nationella lagstiftaren och de nationella myndigheterna som ska bedöma om ett ingripande har varit nödvändigt med avseende såväl på att samhällsbehoven krävt detta som på proportionaliteten (Silver m.fl. mot Förenade kungariket, Handyside mot Förenade kungariket). När de nationella aktörerna genomför denna bedömning finns det en viss prövningsmarginal och hur bred den är avgörs bland annat av vilken av rättigheterna enligt Europakonventionen som ingripandet gäller, hur djupt ingripande det är fråga om och om det syfte som artikel 8.2 i Europakonventionen tillåter är den legitima grunden för ingripandet. Prövningsmarginalen är bredare än vanligt när den legitima grunden är den nationella säkerheten (Klass m.fl. mot Tyskland, Leander mot Sverige). Statens rätt omfattande prövningsrätt gäller också de konkreta medel och metoder som den använder sig av för att skydda den nationella säkerheten. I sitt avgörande Weber och Saravia mot Tyskland ansåg Europadomstolen att staten inom ramen för sin prövningsrätt kunde ha lagstiftat om omfattande övervakning av kommunikationsförbindelser som metod för att skydda den nationella säkerheten. Det var fråga om ett i ett demokratiskt samhälle nödvändigt ingripande i de rättigheter som artikel 8 i Europakonventionen garanterar enskilda rättssubjekt.

I sina nya avgöranden Zakharov samt Szabo och Vissy, som på samma sätt som avgörandet Weber och Saravia gällde underrättelseinhämtning som avser datatrafik, preciserade dock Europadomstolen nödvändighetskriteriet på ett sätt som till viss del verkar reducera statens ovannämnda prövningsrätt. När det är fråga om användningen av sådan övervakningsteknik som hör till det allra senaste inom underrättelseinhämtning som avser datatrafik ska domstolen tolka förutsättningen ”nödvändig i ett demokratiskt samhälle” som att det förutsätts ”absolut nödvändighet” (strict necessity) i två avseenden. För det första ska den hemliga observationsåtgärden rent allmänt vara absolut nödvändig för att skydda de demokratiska institutionerna. För det andra ska åtgärden vara absolut nödvändig för att få fram vital information i samband med en enskild underrättelseinhämtningsoperation.

Europadomstolen har av hävd framhållit att sådana hemliga observations- och övervakningsbefogenheter som myndigheterna använder för att skydda den nationella säkerheten kan utgöra en fara för den demokratiska samhällsordningen (bl.a. Antunes Rocha mot Portugal). Av detta skäl ska staten ordna en oberoende övervakning av hur de används och effektiva rättsmedel. Oberoende övervakning kan lika väl utföras av ett organ bestående av parlamentsledamöter (åtminstone om både regeringspartierna och oppositionen är representerade) som av ett organ bestående av personer som är behöriga att inneha domartjänster, antingen utsedda av parlamentet eller av premiärministern (Klass mot Tyskland, Weber och Saravia mot Tyskland, Leander mot Sverige, L. mot Norge, Kennedy mot Förenade kungariket). I de senaste avgörandena har man framhållit betydelsen av rättslig övervakning som är yrkesmässigt utförd (Szabo och Vissy mot Ungern). Däremot uppfyller en aktör som har alltför nära relationer till den verkställande makten inte kravet på oberoende för övervakaren. Således kan ett system som innebär att en minister utför övervakningen anses strida mot kravet på oberoende – i synnerhet om ministern deltar i beslutsfattandet om användningen av metoderna för informationsinhämtning (Association for European Integration and Human Rights och Ekimdzhiev mot Bulgarien).

De avgöranden som träffas av den aktör som utför övervakningen måste ha en rättsligt bindande verkan på de aktörer som övervakas – med tanke på skyddet för demokratin är det inte

tillräckligt att laglighetsövervakarna kan handleda de aktörer som de övervakar med hjälp av rekommendationer (Segerstedt-Wiberg m.fl. mot Sverige). Den rättsliga regleringen av de hemliga befogenheterna ska vara offentlig och så pass exakt att laglighetsövervakningen kan utföras på ett trovärdigt sätt (Liberty m.fl. mot Förenade kungariket), dock utan att äventyra syftet med den hemliga informationsinhämtningen (Segerstedt-Wiberg m.fl. mot Sverige). Samtidigt bör resultaten av laglighetsövervakningen vara så pass offentliga att medborgarna kan försäkra sig om att systemet för laglighetsövervakning fungerar och är effektivt (Zakharov mot Ryssland). Med tanke på skyddandet av demokratin är det av betydelse att parlamentet deltar i övervakningen av de hemliga observationsbefogenheterna (Campbell mot Förenade kungariket, Leander mot Sverige).

Till kravet på nödvändighet i ett demokratiskt samhälle hör också ett krav på att rättsskydd ska vara tillgängligt nationellt. En domstol i konventionsstaten eller ett motsvarande organ ska åtminstone i efterhand kunna säkerställa att ingripandet i rättigheterna enligt 8 artikeln i Europakonventionen i det enskilda fallet var proportionerligt och nödvändigt. Detta innebär att den som är föremål för informationsinhämtningen ska kunna anföra besvär eller klagan över den åtgärd för informationsinhämtning som riktats mot honom eller henne. En förutsättning för möjligheten till besvär eller klagan är vanligen att personen i fråga får information av myndigheten om den informationsinhämtning som riktats mot honom eller henne när användningen av metoden för informationsinhämtning avslutats (se ovan Zakharov mot Ryssland). Av detta följer dock inte att personen måste underrättas direkt efter att informationsinhämtningen avslutats. Det hot som det inhämtats uppgifter om med hjälp av metoder för informationsinhämtning kan kvarstå i åratal, till och med årtionden, och då är det nödvändigt att på motsvarande sätt skjuta upp denna underrättelse för att skydda säkerhetsmyndigheternas verksamhet. För att göra det möjligt att använda rättsmedel ska underrättelsen ske när det inte längre finns någon specificerad grund för att inte underrätta om saken (Klass mot Tyskland, Zakharov mot Ryssland). Även ett system som inte alls förutsätter att föremålet för åtgärden underrättas kan vara förenligt med Europakonventionen. Då måste det ha föreskrivits så allmänt om rätten att anföra klagan i den nationella lagstiftningen att vem som helst får anföra klagan endast på grund av att han eller hon misstänker att myndigheterna har ingripit i det skydd som han eller hon åtnjuter för sin konfidentiella kommunikation (Kennedy mot Förenade kungariket).

Rätt till ett effektivt rättsmedel

Enligt artikel 13 i Europakonventionen ska var och en, vars i Europakonventionen angivna fri- och rättigheter kränkts, ha tillgång till ett effektivt rättsmedel inför en nationell myndighet och detta även om kränkningen förövats av en person som har handlat i egenskap av offentlig myndighet.

Artikel 13 skiljer sig till sin karaktär från artikel 8 som beskrivits ovan. Artikel 8 gäller självständiga rättigheter, medan artikel 13 endast granskas i förhållande till en sådan bestämmelse i konventionen som anger någon annan rättighet. Artikel 13 kompletterar de andra artiklarna som anger de materiella mänskliga rättigheter som tryggas i konventionen genom att förutsätta effektiva nationella rättsmedel om de här rättigheterna kränks. Bestämmelsen i konventionen kan anses vara ett uttryck för att också de mänskliga rättigheter som skyddas genom internationella konventioner på processuell nivå i första hand ska tryggas inom ramarna för det nationella rättssystemet.

Att artikel 13 som gäller rättsmedel i regel inte kan tillämpas med avseende på de artiklar som gäller rättegångsförfarande har att göra med att det i den, i motsats till artikel 5 (rätt till frihet och säkerhet) och artikel 6 (rätt till en rättvis rättegång), inte nödvändigtvis krävs att det effektiva rättsmedel som avses är en domstol. Vilket nationellt rättsmedel som krävs enligt artikel 13 är snarare beroende av den berörda rättighetens natur och omständigheterna kring varje en-

skilt fall. Bestämmelsen i artikel 13 förutsätter rättsmedel, men garanterar inte en positiv utgång i själva sakfrågan för den ändringssökande.

Europadomstolen har betonat att det vid tolkningen av artikel 13 måste finnas en viss flexibilitet från fall till fall och att överdriven formalitet ska undvikas. Omständigheterna kring varje enskilt fall har betydelse för domstolens helhetsbedömning, då de formella förutsättningarna i den nationella lagstiftningen och realiteterna i den berörda statens juridiska och politiska system samt ändringssökandens specificerade omständigheter beaktas. Artikel 13 innebär inte heller att ett nationellt organ för ändringssökande uttryckligen ska kunna pröva ett påstående om kränkning av någon annan bestämmelse i Europakonventionen. Det är tillräckligt att ett sådant rättsmedel finns som det i sak varit möjligt att vända sig till för att få frågan om det handlar om ett brott mot konventionen prövad.

I avgörandet Klass m.fl. mot Tyskland som gällde telefonavlyssning konstaterade domstolen att det i sådana fall med effective remedy avses ett så effektivt rättsmedel som möjligt med beaktande av de begränsningar som uppstår naturligt vid hemlig övervakning. Att den som känner sig övervakad under sådana omständigheter i praktiken har en begränsad möjlighet att vända sig till en särskild kommission som övervakar verkställigheten av lagen samt författningsdomstolen har i ljuset av artikel 13 ansetts tillräckligt.

I avgörandet Leander mot Sverige hade den svenska säkerhetspolisen upprättat ett register och utifrån uppgifterna i detta kunde personer som klassificerats som en säkerhetsrisk nekas förordnande till vissa statliga tjänster eller uppdrag. Enligt den svenska regeringen hade en sådan person fyra rättsmedel: 1) möjlighet att söka tjänsten och överklaga beslutet hos regeringen, 2) möjlighet att begära tillstånd av polisstyrelsen för att fördjupa sig i de egna uppgifterna och i samband med detta i sista hand föra det negativa beslutet till Regeringsrätten för prövning, 3) möjlighet att anföra klagan hos justitieombudsmannen; 4) möjlighet att anföra klagan hos justitiekanslern. Domstolen ansåg med rösterna 4-3, att inget av dessa var ett effektivt rättsmedel i enlighet med artikel 13, men att de var att anse som tillräckliga med beaktande av ärendets natur tillsammans med ändringssökandens möjlighet att anföra klagan hos regeringen om polisstyrelsens åtgärder. Efter att domstolen kommit fram till denna slutsats betonade den också den parlamentariska övervakning som hör samman med systemet i fråga i Sverige. Däremot fastställdes att artikel 13 kränkts i fallet Segerstedt-Wiberg m.fl. mot Sverige. Trots att domen inte upphäver de principer som utvecklades vid Leander-avgörandet, visar den ett mer kritiskt förhållningssätt gentemot synsättet att rättsmedlen som en helhet betraktade tillsammans kan vara tillräckligt effektiva, även om inget av dem enskilt eller i sig självt utgör ett effektivt rättsmedel.

Fallet Al-Nashif mot Bulgarien, 20.6.2002 gällde en utvisning av en utlänning av skäl som hade samband med den nationella säkerheten. Ändringssökanden åberopade skäl för att artikel 13 skulle granskas med avseende på skyddet för familjelivet i artikel 8. Även om partens rätt att få kännedom om allt bakgrundsmaterial i sitt fall kan begränsas på grund av statliga säkerhetsintressen, måste en oberoende aktör i sådana fall bedöma ändamålsenligheten i grunderna för förfarandet och säkerställa att kravet på ett kontradiktoriskt förfarande uppfylls i tillräcklig grad. Eftersom den behöriga domstolen inte alls kunde pröva grunderna för myndighetens beslut, ansågs artikel 13 ha kränkts. En liknande situation framkom också i avgörandet C.G. m.fl. mot Bulgarien, 24.4.2008. Där grundade sig en utvisning ur landet på en hemlig rapport av inrikesministeriet enligt vilken ändringssökanden enligt underrättelseinformation deltagit i narkotikabrott. De domstolar som senare behandlade ärendet hade fått kännedom om den hemliga rapporten, men de nöjde sig med uppgifterna i rapporten utan vidare åtgärder för att kontrollera fakta i ärendet och utan att erbjuda ändringssökanden möjligheten att bestrida innehållets riktighet i den hemliga rapporten eller möjligheten att argumentera för grunder som gäller skydd för familjelivet. Även i det här fallet ansågs rättsmedlet stå i strid med artikel 13.

Högsta förvaltningsdomstolen i Finland hänvisade bland annat till Al-Nashif-domen i flera av de beslut som den fattade under sommaren 2017, när det var fråga om partsoffentligheten i utlåtanden med säkerhetsriskbedömningar av skyddspolisen i ärenden som gällde familjeåterföreningar och ansökningar om medborgarskap i enlighet med utlänningslagen. Högsta förvaltningsdomstolen ansåg att utlåtandena kunde hållas hemliga för parterna, men som garanti för ett rättvist förfarande krävdes att domstolen fick uppgifter om grunderna för det negativa utlåtandet som parten fått och att domstolen tog ställning till hur korrekta de här grunderna var.

Ett rättsmedels effektivitet i enlighet med artikel 13 är inte beroende av om det varit framgångsrikt. I avgörandet Vereinigung Demokratischer Soldaten Österreichs och Gubi mot Österrike, 19.12.1994 var det fråga om förbud mot spridning av en dagstidning på ett kasernområde, vilket rörde artikel 10. Regeringen kunde inte visa att den ändringssökande föreningen hade haft tillgång till ett effektivt rättsmedel, varför artikel 13 ansågs ha kränkts. Den andra ändringssökanden som var värnpliktig kunde däremot anföra besvär om kränkning av yttrandefriheten hos författningsdomstolen, vilket han också gjorde. Det att överklagandet var resultatlöst hade ingen betydelse med avseende på artikel 13, varför det till denna del inte skedde någon kränkning.

Europadomstolen har i sin senare rättspraxis krävt effektiva rättsmedel också i fråga om laglighetskontrollen av tvångsmedel som ingriper i hemfriden. I avgörandet Stefanov mot Bulgarien, 22.5.2008 bedömdes rättsskyddgarantierna i samband med husrannsakan utifrån kraven i artikel 13. I det här fallet tillät den nationella lagstiftningen inte att domstolen kontrollerade grunderna och tillvägagångssätten för husrannsakan. I artikel 13 i Europakonventionen förutsätts inte att rättsmedlet ska vara tillgängligt före husrannsakan. Kränkningen av artikel 13 orsakades av att det i det nationella rättssystemet inte fanns något annat rättsligt förfarande där den som var föremål för genomsökningen skulle ha kunnat bestrida lagligheten i genomsökningen och beslaget och få skälig kompensation i det fall att beslutet om genomsökningen och beslaget fattats eller verkställts olagligt.

Rättsmedlets effektivitet kräver att beslutet verkställs. Ett framgångsrikt ändringssökande är som sådant inte tillräckligt för att ett rättsmedel ska vara förenligt med artikel 13 om domstolsavgörandet eller beslutet inte får några konkreta följder. Då det för vissa länder upprepade gånger kommit fram att det förekommer avsevärda fördröjningar i verkställandet av domstolarnas domar och beslut, har Europadomstolen i sin rättspraxis betonat att det i det nationella rättssystemet måste finnas tillräckliga rättsskyddsgarantier mot den här typen av fördröjningar.

2.5 Europeiska unionens stadga om de grundläggande rättigheterna

Europeiska unionens stadga om de grundläggande rättigheterna, som trädde i kraft 2009, fastställer de grundläggande rättigheter som gäller inom unionen. Medlemsstaterna är skyldiga att följa stadgan varje gång de tillämpar unionsrätten. Enligt artikel 7 i stadgan har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Enligt artikel 8 i stadgan har var och en också rätt till skydd av de personuppgifter som rör honom eller henne. Uppgifter som omfattas av skyddet av personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Artikel 52 i stadgan fastställer räckvidden för de rättigheter som tryggas genom stadgan. Enligt artikel 52.1 ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och

friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter. I den mån som stadgan omfattar rättigheter som motsvarar sådana som garanteras av europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna ska de enligt artikel 52.3 ha samma innebörd och räckvidd som i konventionen. Detta hindrar emellertid inte unionsrätten från att tillförsäkra ett mer långtgående skydd.

Av artikel 52.3 i stadgan följer att innehållet i artikel 7 i stadgan ska motsvara innehållet i artikel 8 i Europakonventionen. I ingressen till stadgan konstateras det särskilt att de rättigheter som bekräftas har sin grund både i Europakonventionen och i Europadomstolens avgörandepraxis. Dessa ska alltså också anses vara relevanta för tolkningen av artikel 7 i stadgan.

Europeiska unionens domstols avgörandepraxis

Anknytning till och tillämpning av EU-rätten

Bestämmelserna i EU:s stadga om de grundläggande rättigheterna (EUT C 326, 26.10.2012) riktar sig enligt artikel 51.1 i stadgan, med beaktande av subsidiaritetsprincipen, till unionens institutioner, organ och byråer samt till medlemsstaterna endast när dessa tillämpar unionsrätten. Stadgan tillämpas alltså inte i situationer där det är fråga om tillämpning av enbart nationell lagstiftning och som inte regleras i EU-rätten. Även i situationer som inte omfattas av EU-rätten kan stadgan emellertid erbjuda tolkningshjälp, till exempel om Europadomstolen inte har behandlat en viss rättighet eller fråga som ansluter sig till en rättighet, men det finns rättspraxis om saken hos EU-domstolen.

För att EU-rätten ska vara tillämplig i ett visst ärende krävs det att ärendet har ”tillräcklig anknytning” till EU-rätten (beslut Burzio, C-497/14, punkterna 28–31; beslut Văraru, C-496/14, punkt 21; beslut Petrus, C‑451/14, punkterna 18–20). Enbart existensen av EU:s behörighet räcker inte för att ett ärende ska omfattas av tillämpningsområdet för EU-rätten, utan det som har betydelse är om unionen har använt sin behörighet till att utfärda bestämmelser som gäller ärendet. EU:s grundläggande rättigheter eller allmänna rättsprinciper som sådana, utan någon konkret anknytning till EU-rätten, utgör inte någon sådan tillräcklig anknytning som avses här och gör då inte heller att ett ärende ska omfattas av EU-rätten (beslut Pondiche, C-608/14, punkt 21; dom Torralbo Marcos, C-265/13, punkt 30; dom Pelckmans Turnhout, C-483/12, punkt 20; beslut Balázs och Papp, C-45/14, punkt 23; dom Åkerberg Fransson, C-617/10, punkt 22; beslut Nagy m.fl., C-488/12–C-491/12 och C-526/12, punkt 17; beslut Cholakova, C-14/13, punkt 30).

Av betydelse vid bedömningen av huruvida EU-rätten ska tillämpas i anslutning till lagstiftningen om underrättelseinhämtning är de undantag som finns i EU-lagstiftningen och med stöd av vilka tillämpningen av EU-rätten har begränsats i flera rättsakter så att den inte omfattar ärenden som gäller nationell säkerhet. Undantagen grundar sig på den bestämmelse som finns i artikel 3.2 i fördraget om Europeiska unionen och enligt vilken den nationella säkerheten också i fortsättningen ska vara varje medlemsstats eget ansvar. Unionen har således åtminstone ingen direkt behörighet när det gäller nationell säkerhet. Artikeln i fråga innehåller emellertid ingen definition av var exakt gränsen mellan EU:s behörighet och den nationella behörigheten går. EU-rätten omfattar ett stort antal områden som har direkt eller indirekt betydelse inom den nationella säkerhetens och den allmänna ordningens område. Samtidigt erkänns den nationella dimensionen av dessa intressen i och med att de nämns i flera artiklar i EU-fördragen och i flera EU-rättsakter såsom grunder för undantag eller legitima grunder när det gäller EU:s samarbetsområden. I praktiken är det alltså inte alltid entydigt att utesluta tillämpningsområdet för EU-rätten på grundval av undantaget i fråga om nationell säkerhet. En

medlemsstat som åberopar nationell säkerhet som grund måste också påvisa ett verkligt behov av att ty sig till en sådan grund (dom ZZ, C-300/11; dom Insinööritoimisto InsTiimi Oy, C-615/10, punkt 35; dom kommissionen mot Finland, C-284/05, punkterna 45 och 47).

Skydd för hemligheten i fråga om förtroliga meddelanden

En bestämmelse om skydd för hemligheten i fråga om förtroliga meddelanden finns i artikel 7 i EU:s stadga om de grundläggande rättigheterna. Enligt artikeln har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Enligt artikel 8 i stadgan har var och en också rätt till skydd av de personuppgifter som rör honom eller henne.

Betydelsen av de grundläggande rättigheter som gäller respekten för privatlivet och skyddet av personuppgifter betonas i EU-domstolens rättspraxis, i synnerhet i samband med elektronisk kommunikation (bl.a. dom Tele2 Sverige AB och Secretary of State for the Home Department, förenade målen C-203/15 och C-698/15, punkt 93, Schrems, C-362/14, punkt 39; dom Rijkeboer, C-553/07, punkt 47; dom Digital Rights Ireland m.fl., punkt 53 och dom Google Spain och Google, C-131/12, punkterna 53, 66 och 74 och där angiven rättspraxis).

De förklaringar som gäller stadgan om de grundläggande rättigheterna ska enligt artikel 6.1 tredje stycket i fördraget om Europeiska unionen och artikel 52.7 i stadgan beaktas vid tolkningen av stadgan. Enligt de förklaringar som gäller stadgan (EUT C 303, 14.12.2007, s. 17–35) motsvarar de rättigheter som garanteras i artikel 7 i stadgan de rättigheter som garanteras i artikel 8 i Europakonventionen och de har samma innebörd och räckvidd. Med hänsyn till den tekniska utvecklingen har ordet ”kommunikationer” i Europakonventionen ersatts med ”korrespondens” i artikel 7 i stadgan.

I artikel 52.3 i stadgan fastställs det att i den mån som stadgan omfattar rättigheter som motsvarar sådana som garanteras i Europakonventionen ska de ha samma innebörd och räckvidd som i konventionen. Denna bestämmelse hindrar inte unionsrätten från att tillförsäkra ett mer långtgående skydd.

Bestämmelsen i artikel 52.3 i stadgan som gäller skydd som är mer långtgående än i Europakonventionen innebär att nivån på det skydd som fastställs i stadgan aldrig får vara lägre än motsvarande nivå i konventionen, men den får vara högre. Vid tolkningen av innehållet i och nivån på skyddet för de grundläggande rättigheter som erkänns i EU:s rättsordning ska man först och främst stödja sig på EU-domstolens rättspraxis i fråga om en viss rättighet (yttrande om EU:s anslutning till Europakonventionen, 2/13, EU:C:2014:2454, punkt 170; dom Kadi och Al Barakaat, C-402/05 och C-415/04 P, punkterna 281–285; dom Internationale Handelsgesellschaft, C-11/70, punkt 4).

De rättigheter och friheter som erkänns i EU:s stadga om de grundläggande rättigheterna är i regel inte ovillkorliga, utan utövandet av dem kan begränsas. Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Enligt EU-domstolens rättspraxis ska den rättsliga grunden för en begränsning, i enlighet med kravet på bestämmelser i lag, bland annat vara tillräckligt klar och precis och den måste ge ett visst skydd mot eventuella ingrepp (dom WebMind, C-419/14, punkt 81). Detta kriterium påminner nära om det som på motsvarande sätt fastställs i Europakonventionen om att villkoren för en begränsning av rättigheter ska vara föreskrivna i lag. Därför kan Europadomstolens

rättspraxis erbjuda tolkningshjälp för detta kriterium i synnerhet när det gäller sådana bestämmelser i stadgan som motsvarar rättigheter som ingår i Europakonventionen.

Av EU-domstolens rättspraxis framgår bland annat att ”bekämpandet av grov brottslighet i syfte att garantera allmän säkerhet” (dom Tsakouridis, C-145/09, punkterna 46 och 47) och ”bekämpandet av internationell terrorism i syfte att upprätthålla internationell fred och säkerhet” (dom WebMind, C-419/14, punkt 76; dom Kadi och Al Barakaat, C-402/05 P och C-415/05 P, punkt 363 och dom Al-Aqsa mot rådet, C-539/10 P och C-550/10 P, punkt 130) är mål som är förenliga med unionens allmänna samhällsintresse. Dessutom nämns ”nationell säkerhet” uttryckligen i artikel 4.2 i fördraget om Europeiska unionens funktionssätt och har av tradition godtagits i EU-domstolens rättspraxis som ett mål som berättigar till begränsningar av de grundläggande rättigheterna (t.ex. dom kommissionen mot Finland, C-284/05, punkterna 45, 47 och 49).

I EU-domstolens praxis har bedömningen av huruvida begränsningar av de grundläggande rättigheterna följer proportionalitetsprincipen ofta visat sig vara det avgörande steget i bedömningen. Den proportionalitetsprincip som nämns i artikel 52.1 i stadgan hör till EU-rättens allmänna principer och kräver enligt EU-domstolens etablerade rättspraxis att de berättigade målen för den åtgärd eller författning som ska bedömas kan genomföras med hjälp av de medel som föreskrivits av unionen och att de inte överskrider vad som är behövligt och nödvändigt för att målen ska nås samt vad som är lämpligt (appropriate and necessary, t.ex. dom Schaible, C-101/12, punkt 29; dom Sky Österreich, C-283/11, punkt 50; dom Nelson m.fl. C-581/10 och C-629/10, punkt 71; dom Volker und Markus Schecke, C-92/09 och C-93/09, punkt 74 och dom Afton Chemical, C-343/09, punkt 45).

I praktiken handlar det om att hitta en godtagbar balans mellan olika intressen. Undantag och begränsningar som gäller en grundläggande rättighet ska vara nödvändiga så att åtgärderna innebär ett så litet ingrepp som möjligt i rättigheten samtidigt som man effektivt bidrar till att målen med den aktuella EU-regleringen nås (dom WebMind, punkt 82; dom Schecke, punkterna 87 och 88; dom R., C-285/09, punkt 45).

När EU-domstolen har gjort bedömningar enligt proportionalitetsprincipen i ärenden som gällt integritetsskydd har domstolen ägnat uppmärksamhet åt bland annat tillsynen över det arrangemang som ska bedömas (Tele2 Sverige AB och Secretary of State for the Home Department, punkt 123 och Schrems, punkt 40), att det finns tillräckliga rättsmedel (bl.a. Schrems, punkt 95 och UGT-Rioja m.fl., C-428/06–C-434/06, punkt 80), uppgiftslämning och informationssäkerhet samt villkoren i fråga om de personer som berörs, förhandstillstånd (dom WebMind, punkterna 77 och 78), tillgång till uppgifter, uppgifternas förvaringstid och förstöring av uppgifter (Tele2 Sverige AB och Secretary of State for the Home Department, punkt 122 och dom Digital Rights Ireland, punkterna 56–67).

Riksdagens grundlagsutskott framförde i sitt utlåtande GrUU 18/2014 rd vissa observationer i fråga om EU-domstolens dom i målet Digital Rights Ireland m.fl., dvs. den så kallade data retention-domen. Enligt utskottet ger domen inget direkt svar på hur den nationella lagstiftningen ska utformas för att uppfylla kraven på proportionalitet när det gäller privatlivet och personuppgifter. Man måste enligt utskottet dock utgå från att åtminstone sådana bestämmelser strider mot proportionalitetskravet som innebär omfattande, ospecificerad, långvarig och obegränsad förvaring av uppgifter i kombination med att myndigheter har ospecificerad och obegränsad tillgång till dessa uppgifter. Grundlagsutskottet konstaterade också att det på basis av domen förblir öppet huruvida det att skyldigheten att lagra uppgifter för myndigheternas behov i praktiken utsträcker sig till uppgifter om alla personer som använder elektroniska kommunikationsmedel i sig innebär en kränkning av proportionalitetskravet.

I sin dom konstaterade EU-domstolen att direktivet hade behövt innehålla objektiva gränser i anslutning till dess mål i fråga om vilka personers identifieringsuppgifter som får lagras. Dessutom borde det i direktivet närmare ha definierats vilka brott som skulle bekämpas med hjälp av skyldigheten att lagra uppgifter. Till denna del är det viktigt att vara medveten om att EU-domstolens dom egentligen inte skapar någon ny rätt. Den motsvarar Europadomstolens etablerade avgörandepraxis. Europadomstolen har meddelat ett ganska stort antal avgöranden där den på ett sätt som motsvarar EU-domstolens dom, men mera detaljerat, har behandlat de element som en lag som ingriper i skyddet för privatlivet ska innehålla för att vara förenlig med proportionalitetsprincipen och förutsägbar. Bland de viktigaste avgörandena i detta sammanhang är de av Europadomstolens avgöranden som direkt har gällt underrättelseinhämtning som avser datatrafik eller närliggande fenomen, såsom Klass mot Tyskland (1978), Weber och Saravia mot Tyskland (2006) och Liberty m.fl. mot Förenade kungariket (2008).

EU-domstolen har behandlat kravet på respekt för det väsentliga innehållet i grundläggande rättigheter i sitt avgörande Schrems. Enligt domstolen måste en lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer i synnerhet anses kränka det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet (punkt 94). Dessutom konstaterade domstolen att en lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem inte respekterar det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd (punkt 95).

2.6 Bedömning av nuläget

Allmänt

De myndigheter som ansvarar för den nationella säkerheten ska förutse och inhämta information om sådan verksamhet som kan äventyra eller hota sådana nationella intressen som uppfattas som särskilt viktiga. Dessa myndigheter bedriver sådan underrättelseinhämtning som krävs för skötseln av deras lagstadgade uppgifter. Lagstiftningen innehåller emellertid inga befogenheter som gäller underrättelseinhämtning.

Ett gemensamt drag för de uppgifter som sköts av de myndigheter som ansvarar för den nationella säkerheten är att de gäller avvärjande av hot. Avvärjandet av hot förutsätter att hoten kan upptäckas och att man får information om dem i ett tillräckligt tidigt skede. Förutom att förhindra, avslöja och i mindre utsträckning utreda brott har skyddspolisen till uppgift att bekämpa förehavanden som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet. Begreppet förehavanden preciseras inte i polisförvaltningslagen eller i förarbetet till den. När det gäller förehavanden kan man inte anse att det är fråga om brott, vilket betyder att myndighetens uppdrag till denna del gäller underrättelseinhämtning och inte brottsbekämpning.

Det finns inte heller några bestämmelser om befogenheter för underrättelseinhämtning för de myndigheter som avvärjer hot mot den nationella säkerheten och hur sådana befogenheter ska fördela sig mellan de civila och militära myndigheterna. I den gällande lagstiftningen grundar sig myndigheternas befogenheter i fråga om informationsinhämtning inte på underrättelseinhämtning utan enbart på brottsbekämpning. Osäkerhetsfaktorerna i anslutning till den förändrade säkerhetsmiljön framhäver behovet av att ta fram objektiv, bekräftad och analyserad information om de säkerhetshot som riktar sig mot Finland till stöd för både det politiska beslutsfattandet och säkerhetsmyndigheternas beslutsfattande. Endast sådan information om avsikterna och planerna hos de aktörer som ligger bakom hoten som är sann och som fås i ett så tidigt skede som möjligt garanterar att det finns tillräcklig förmåga att kunna varna om hoten i

förväg. Tidig information förbättrar det finländska samhällets möjligheter att förbereda sig på hot och utvidgar det urval av medel med vars hjälp en realisering av hoten kan förhindras.

Den nuvarande situationen kan anses vara otillfredsställande med beaktande av de förändringar som har skett i säkerhetsmiljön. Det finländska samhällets funktionsduglighet måste skyddas mot särskilt allvarliga yttre hot och gärningar som riktar sig mot kritisk infrastruktur. Ur den nationella säkerhetens perspektiv är det väsentligt att man i ett tillräckligt tidigt skede får information om förändringar som sker i Finlands säkerhetsmiljö. Det är av största vikt att man får in information om den situation som råder och analyserar dess betydelse för den nationella säkerheten i Finland.

I alla de stater som ingår i den internationella jämförelsen föreskrivs det om underrättelseinhämtning på samma sätt som i de flesta av de suveräna stater med västerländsk demokrati som inte ingår i jämförelsen. Lagstiftningen om underrättelseinhämtning kan innehålla bestämmelser om informationsinhämtning via datanätsmiljöer. Bestämmelsernas exakthet varierar från land till land. Därför är det inte möjligt att dra några direkta slutsatser av lagstiftningen i alla de stater som ingick i jämförelsen när det gäller enskilda metoder för informationsinhämtning som används. Det finns också skillnader i hur exakt de hot som man vill avvärja med hjälp av informationsinhämtningen har definierats i lag.

För underrättelseverksamheten i de stater som ingick i jämförelsen ansvarar antingen en underrättelsemyndighet eller så delas behörigheten mellan civila och militära underrättelsetjänster. Uppdelningen av befogenheterna för underrättelseinhämtning mellan civila och militära myndigheter grundar sig i regel på om hotet är av civil eller militär art. Underrättelsetjänsterna leds och styrs i allmänhet av försvarsministeriet, inrikesministeriet eller bägge två. De uppdrag som gäller informationsinhämtning kan komma från statsledningen, de styrande ministerierna eller till exempel ledningen för försvarsmakten.

Skyddspolisens uppgifter

Skyddspolisen är en riksomfattande polisenhet som lyder under inrikesministeriet och som enligt 10 § 1 mom. i polisförvaltningslagen har till uppgift att i enlighet med inrikesministeriets styrning bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet samt att utföra undersökning av sådana brott. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att förebygga verksamhet som äventyrar rikets säkerhet.

När det gäller 10 § i polisförvaltningslagen var avsikten enligt regeringens proposition RP 155/1991 rd att man genom det sätt på vilket bestämmelsen är skriven skulle beakta den accentuerade betydelsen av förebyggande verksamhet inom skyddspolisens uppgiftsområde. Enligt förarbetet har förebyggandet av handlingar som äventyrar rikets säkerhet en mycket central ställning i skyddspolisens arbete, medan om en redan inträffad kränkning av säkerhetsintressena är föremål för undersökning är detta i allmänhet ett bevis för att den förebyggande verksamheten misslyckats i en viss utsträckning. Genom det sätt på vilket bestämmelsen är skriven var avsikten att beakta den accentuerade betydelsen av förebyggande verksamhet inom skyddspolisens uppgiftsområde.

I denna proposition föreslås det att de befogenheter som kan användas i den operativa verksamheten ändras samt föreslås det bestämmelser om informationsinhämtning som avser utländska förhållanden. Till följd av detta kommer alltså ett verksamhetssätt som baserar sig på informationsinhämtning och underrättelseinhämtning att accentueras ytterligare i skyddspolisens verksamhet. Skyddspolisens uppdrag behöver ses över och preciseras så att dess uppgift när det gäller underrättelseinhämtning och informationsinhämtning framgår tydligare, med be-

aktande av de befogenheter som föreslås i lagstiftningen och det att skyddspolisen själv aktivt ska börja inhämta information som avser utländska förhållanden. Karaktären av underrättelseinhämtning kan beskrivas genom att man i skyddspolisens uppdrag betonar karaktären av informationsinhämtning när det gäller att skydda den nationella säkerheten samt genom att varsebli sådana aktiviteter, förehavanden eller brott som kan hota samhällsordningen eller rikets inre eller yttre säkerhet. Skyddet av den nationella säkerheten behöver också nämnas i den bestämmelse om polisens uppgifter som finns i 1 kap. 1 § 1 mom. i polislagen eftersom det i fråga om skyddet av den nationella säkerheten också kommer att finnas en uppgift som mera allmänt hör till polisen, även om skyddspolisen kommer att vara den enda polisenheten som kan använda sig av underrättelseinhämtningsmetoder för att inhämta information om verksamhet som utgör ett allvarligt hot mot den nationella säkerheten.

Nationell säkerhet nämns uttryckligen i artikel 4.2 i fördraget om Europeiska unionens funktionssätt och har av tradition godtagits i EU-domstolens rättspraxis som ett mål som berättigar till begränsningar av de grundläggande rättigheterna. Det är en av de grunder som enligt artikel 8 i Europakonventionen kan berättiga till ett ingripande i skyddet för privatlivet. Detta behandlas närmare i avsnitt 2.4 och 2.5 i propositionen.

I de högsta laglighetsövervakarnas avgörandepraxis (t.ex. riksdagens biträdande justitieombudsmans beslut 29.11.2013, dnr 1870/2013 och 18.12.2003, dnr 1634/4/01) konstateras det att bestämmelserna om uppgiftsdefinitionen ändå inte är bestämmelser om befogenheter. Bestämmelsen om uppgifterna ger alltså inte polisen befogenheter att vidta vilka åtgärder som helst när uppgifterna i fråga ska utföras och polisen får alltså inte enbart med stöd av bestämmelsen ingripa i människors i lag skyddade rättigheter. När polisen ingriper i en persons rättsområde ska befogenheten alltid grunda sig på en uttrycklig bestämmelse. På så sätt påvisar inte skyddet av den nationella säkerheten i sig något annat än att skyddspolisen har ett lagenligt och samhälleligt önskvärt motiv för sitt förfarande. Detta berättigar alltså ännu i sig inte att man ingriper i människors grundläggande rättigheter, utan i så fall krävs det en behörighetsregel i lag.

Å andra sidan är det också skäl att beakta grundlagens 22 §, enligt vilken det allmänna ska se till att de grundläggande fri- och rättigheterna och de mänskliga rättigheterna tillgodoses. Denna paragraf innebär också skyldighet för polisen att utöva sina befogenheter. Denna synpunkt understryks också i Europadomstolens avgörandepraxis. Till exempel i avgörandet Kontrova mot Slovakien 31.5.2007 var det fråga om myndigheternas positiva skyldighet att vidta konkreta förebyggande åtgärder för att skydda en person vars liv var i fara på grund av en annan persons brottsliga handlingar. Inom ramen för befogenheterna ska sådana åtgärder vidtas som på ett rationellt sätt är ägnade att avvärja sådan fara. Frågan om polisens skyldighet att trygga de grundläggande fri- och rättigheterna och mänskliga rättigheterna samt om metoderna för detta behandlas också i till exempel avgörandena Surugiu mot Rumänien 20.4.2004, Ouranio Toxo m.fl. mot Grekland 20.10.2005 och Babylonova mot Slovakien 20.6.2006 (RP 224/2010 rd, s. 75).

Skyddspolisens befogenheter

Hemliga metoder för inhämtande av information

I sitt uppdrag använder sig skyddspolisen av sådana hemliga metoder för inhämtande av information som det föreskrivs om i 5 kap. i polislagen: teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk observation (teknisk avlyssning, optisk observation, teknisk spårning och teknisk observation av utrustning), inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevispro-

vokation genom köp, användning av informationskällor och kontrollerade leveranser i syfte att förhindra, avslöja eller avvärja risk för brott.

De hemliga metoder för inhämtade av information som nämns i polislagens 5 kap. kan antas vara användbara och effektiva även vid underrättelseinhämtning och de utgör en god utgångspunkt för befogenheterna för underrättelseinhämtning. Kännetecknande för de hemliga metoderna är att de används utan att målpersonen vet om det. Bestämmelserna i polislagens 5 kap. beaktar även aspekter i fråga om grundläggande och mänskliga rättigheter, vilket bland annat inbegriper att en domstol deltar i beslutsfattandet.

Det är motiverat att polislagens nya 5 a kap. om hemlig informationsinhämtning med avseende på metoderna baseras på bestämmelserna i 5 kap. om hemliga metoder för inhämtande av information. Förutom det som redan har nämnts beror detta på att de metoder som det ska föreskrivas om är desamma, vilket betyder att aspekterna vad gäller konsekvens och ändamålsenlighet talar för att definitionerna och förfaringssätten när det gäller underrättelseinhämtningsmetoder, såsom bestämmelserna om beslutsfattande, så långt som möjligt bör vara desamma. Detta innebär att man när det gäller polislagens 5 a kap. bör avvika från bestämmelserna i 5 kap. endast då det finns grundad anledning till det med tanke på underrättelseverksamhetens särdrag.

Med förhindrande av brott avses enligt 5 kap. 1 § 2 mom. i polislagen åtgärder som syftar till att förhindra brott, försök till brott och förberedelse till brott, när det utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet finns grundad anledning att anta att personen i fråga kommer att göra sig skyldig till brott, samt åtgärder som syftar till att avbryta ett redan påbörjat brott eller begränsa den direkta skada eller fara som brottet medför. Med iakttagelser av en persons verksamhet eller annan information om en persons verksamhet avses direkta iakttagelser av en persons egen verksamhet och tips från utomstående, såsom informationskällor, samt andra indirekta utredningar. Till iakttagelser och annan information räknas också bland annat information som fåtts genom kriminalunderrättelseverksamhet, iakttagelser i samband med observation, andra former av tips och slutsatser som dras på basis av brottsanalyser. Villkoret för att en metod för informationsinhämtning som föreskrivits i syfte att förhindra brott ska få användas är att det på basis av sådan här information med fog kan antas att en person har gjort sig skyldig till brott (RP 224/2010 rd, s. 93). Med avslöjande av brott avses åtgärder som syftar till att klarlägga om det för inledande av förundersökning finns en i 3 kap. 3 § 1 mom. i förundersökningslagen avsedd grund, när det utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet kan antas att ett brott har begåtts.

Med avslöjande av brott avses enligt 5 kap. 1 § 3 mom. i polislagen åtgärder som syftar till att klarlägga om det för inledande av förundersökning finns en i 3 kap. 3 § 1 mom. i förundersökningslagen avsedd grund, när det utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet kan antas att ett brott har begåtts. Begreppet avslöjande av brott syftar till den gråzon som finns mellan förhindrandet och utredningen av brott. Det är inte fråga om brottsutredning eftersom förutsättningar för att inleda en förundersökning saknas, och inte heller förhindrande av brott eftersom brottet antas redan ha blivit begånget. Vid avslöjande av brott är det fråga om till exempel en situation där man har fått tips om att ett brott redan har begåtts, men där det ännu inte finns någon konkret grund för misstanke, det vill säga att tröskeln ”skäl att misstänka” enligt förundersökningslagen ännu inte har överskridits (RP 224/2010 rd, s. 93).

De hemliga metoderna för inhämtande av information ger inte möjlighet att tillräckligt effektivt och i ett tillräckligt tidigt skede upptäcka hot eller vidta de åtgärder som krävs eftersom användningen av sådana metoder är knuten till begreppet brott i lagstiftningen (förhindrande

eller avslöjande av brott). För att man ska kunna identifiera och avvärja hot som eventuellt riktar sig mot Finland och dess befolkning är det nödvändigt att man med stöd av egna befogenheter för skyddspolisen kan inhämta information om verksamhet som allvarligt hotar den nationella säkerheten samt skydda och upprätthålla den nationella säkerheten. Den verksamhet som är föremål för informationsinhämtningen är i många fall inte kriminaliserad eller har inte gått så långt att man kan rikta en konkret och individualiserad brottsmisstanke mot den. Informationsbehovet gäller till exempel säkerhetsmiljöns utveckling och verksamhet som allvarligt hotar statsordningen eller samhällets grundfunktioner, såsom verksamhet som är kopplad till terrorism, våldsam radikalisering och utländska underrättelsetjänsters verksamhet.

Den nationella säkerheten är en av de grunder som enligt artikel 8 i Europakonventionen kan berättiga till ett ingripande i skyddet för privatlivet. Staterna har en ganska bred marginal för skönsmässig bedömning när det gäller vilken typ av verksamhet som de anser äventyrar den nationella säkerheten. På basis av Europadomstolens avgörandepraxis inbegrips åtminstone det militära försvaret, bekämpningen av terrorism och bekämpningen av olaglig underrättelseverksamhet i den nationella säkerheten. Den nationella säkerheten kan emellertid hotas på många olika sätt, och hoten kan vara svåra att förutse eller definiera i förväg. Av detta följer enligt domstolen att klargörandet av begrepp i första hand ska överlåtas till nationell praxis (Kennedy mot Förenade kungariket, 18.5.2010).

Enligt den arbetsgrupp för en informationsanskaffningslag som har bedömt riktlinjerna för underrättelselagstiftningen är det nödvändigt att det för underrättelseverksamheten införs bestämmelser om personbaserad underrättelseinhämtning som avser utländska förhållanden, underrättelseinhämtning som avser utländska datasystem och underrättelseinhämtning som avser datatrafik. Underrättelseinhämtning som avser utländska förhållanden används som gemensam benämning på de första två typerna av underrättelseinhämtning.

Det skulle vara motiverat att användningen av sådana underrättelseinhämtningsmetoder som avser utländska förhållanden skulle vara möjlig även vid underrättelseinhämtning inom landet. Ju närmare en verksamhet som allvarligt hotar den nationella säkerheten pågår, desto nödvändigare är det att få information om den och att sträva efter att förhindra den från att gå vidare till en icke-önskvärd fas. Någon annan lösning skulle vara absurd eftersom bestämmelser om enbart underrättelseinhämtning som avser utländska förhållanden skulle leda till en situation där den finländska underrättelsemyndigheten måste sluta använda sig av sina befogenheter för underrättelseinhämtning utanför Finlands gränser och låta det objekt som man följer komma in i landet, där objektet inte skulle kunna följas på grund av att det saknas befogenheter. När begreppen personbaserad underrättelseinhämtning och underrättelseinhämtning som avser datasystem används i fortsättningen syftar de följaktligen på både underrättelseinhämtning inom landet och underrättelseinhämtning som avser utländska förhållanden.

Med personbaserad underrättelseinhämtning avses sådan underrättelseinhämtning som grundar sig på personlig interaktion eller personliga iakttagelser av en person eller något annat objekt. Med beaktande av kravet på exakthet och noggrann avgränsning i bestämmelserna om befogenheter skulle det vara svårt att lagstifta om så här omfattande befogenheter. Därför måste bestämmelserna om metoder för personbaserad underrättelseinhämtning formuleras med beaktande av de gällande ramarna för befogenhetsbestämmelser. Området för personbaserad underrättelseinhämtning ska åtminstone omfatta teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, delvis teknisk avlyssning, optisk observation, teknisk spårning, inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp och användning av informationskällor.

Med underrättelseinhämtning som avser datasystem avses sådan underrättelseinhämtning som sker med datatekniska metoder och som gäller uppgifter som behandlas i datasystem. Detta motsvaras såsom teknisk observation av teknisk observation av utrustning och delvis teknisk avlyssning.

Bestämmelser om befogenheter för underrättelseinhämtning kunde ingå i det nya 5 a kap. i polislagen. Befogenheterna kunde benämnas underrättelseinhämtningsmetoder, och dessa metoder ska metodmässigt och definitionsmässigt vara samma metoder för inhämtande av information som de som det föreskrivs om i polislagens 5 kap. Förutsättningarna för att sådana här underrättelseinhämtningsmetoder ska få användas ska inte vara desamma som för hemliga metoder för inhämtande av information. På så sätt ska det inte ske någon sammanblandning med begreppen hemliga metoder för inhämtande av information och hemliga tvångsmedel.

Förutsättningarna för användning av hemliga metoder för inhämtande av information

Allmänna och särskilda förutsättningar

En allmän förutsättning för användning av hemliga metoder för inhämtande av information är enligt 5 kap. 2 § 1 mom. i polislagen att man med metoden kan antas få sådan information som behövs för förhindrande, avslöjande eller avvärjande av risk för brott. Utöver vad som i övrigt föreskrivs om särskilda förutsättningar för användning av hemliga metoder för inhämtande av information anges det i 2 mom. i samma paragraf som en ytterligare allmän förutsättning för att teleavlyssning, inhämtande av information i stället för teleavlyssning, systematisk observation, teknisk avlyssning, teknisk spårning av personer, teknisk observation av utrustning, täckoperationer, bevisprovokation genom köp, styrd användning av informationskällor och kontrollerade leveranser ska få användas att dessa metoder kan antas vara av synnerlig vikt för förhindrande eller avslöjande av ett brott. För täckoperationer och bevisprovokation genom köp förutsätts det dessutom att användningen av metoden är nödvändig för att ett brott ska kunna förhindras eller avslöjas.

Polislagen innehåller så kallade allmänna och särskilda förutsättningar för användningen av olika metoder för inhämtning av information. Särskilda förutsättningar för användningen av hemliga metoder för inhämtande av information är framför allt de specificerade brott som man strävar efter att förhindra med hjälp av de olika metoderna. I bestämmelserna om olika metoder för informationsinhämtning kan det också ingå andra särskilda förutsättningar. Sammanfattningsvis kan det konstateras att skyddspolisen på ett nästan heltäckande sätt kan använda de hemliga metoder för inhämtande av information som det föreskrivs om i 5 kap. i polislagen för att förhindra sådana terroristbrott som är straffbara enligt 34 a kap. i strafflagen och sådana brott i anslutning till olaglig underrättelseverksamhet som är straffbara enligt 12 kap. i strafflagen. När det gäller förhindrande av brott som syftar till att sprida massförstörelsevapen och produkter med dubbel användning, liksom brott som är kopplade till organiserad brottslighet och som äventyrar statens säkerhet, är situationen mera mångfasetterad och svårtolkad.

De ovan nämnda hemliga metoderna för inhämtande av information får användas för avslöjande av brott endast då det är fråga om ett sådant landsförräderibrott eller terroristbrott som det föreskrivs närmare om i lagen. I fråga om avslöjande av brott tillämpas inte de särskilda förutsättningar som anges i de metodrelaterade bestämmelserna om hemliga metoder för inhämtande av information (RP 224/2010 rd, s. 95).

Det bör tas in motsvarande bestämmelser i polislagens 5 a kap., där användningen av metoder för underrättelseinhämtning graderas i enlighet med hur kännbart de ingriper i de grundläggande rättigheterna och mänskliga rättigheterna för objektet. I detta sammanhang kan även de förväntningar på resultatet och formuleringarna ”av synnerlig vikt” och ”nödvändig” som re-

dan ingår i det nuvarande 5 kap. få gälla. Syftet med användningen av underrättelseinhämtningsmetoder är inte att förhindra, avslöja eller utreda brott utan att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten. Sådan verksamhet ska definieras så detaljerat som över huvud taget är möjligt. Vad gäller enskilda åtgärder bör bestämmelserna om andra förutsättningar för att använda metoderna även här vara så exakta och noggrant avgränsade som möjligt. Detta gäller till exempel i fråga om vem som användningen av befogenheter får riktas mot eller giltigheten för ett tillstånd eller beslut.

Målet med användningen av de metoder för underrättelseinhämtning som föreslås i polislagens 5 a kap. är att få information om verksamhet som allvarligt hotar den nationella säkerheten. I polislagen bör det ingå en definition av vad som avses med verksamhet som allvarligt hotar den nationella säkerheten. Eftersom verksamhet som äventyrar den nationella säkerheten inte utgör förhindrande, avslöjande eller utredning av brott och verksamheten kan vara sådan att den om den konkretiseras aldrig kommer att utgöra ett brott, bör underrättelsemyndigheten ha möjlighet att med låg tröskel kunna börja inhämta information om sådan verksamhet som allvarligt hotar den nationella säkerheten. I så fall kan det med fog fastslås att förutsättningen för att metoder för underrättelseinhämtning ska få användas är att informationsinhämtningen ska gälla de allra största hoten ur samhällets perspektiv. Hot mot den nationella säkerheten (objekt för civil underrättelseinhämtning) behandlas närmare i detaljmotiveringen till 5 a kap. 3 § i förslaget till polislag.

Samhällsfunktionernas sårbarhet och konsekvenserna av skador accentueras i det moderna informationssamhället. Tillgången till riktig information och en tillförlitlig lägesbild över de hot som riktas mot Finlands nationella säkerhet skapar förutsättningar för kontroll av hoten och beslut vid rätt tidpunkt. Den behöriga myndigheten bör ha det operativa ansvaret vid inhämtningen av information.

Brottet och en angiven person

Enligt 5 kap. 3 § i polislagen har skyddspolisen rätt att använda hemliga metoder för inhämtande av information inte bara för att förhindra brott utan även för att avslöja följande brott: 1) äventyrande av Finlands suveränitet, 2) krigsanstiftan, 3) landsförräderi, grovt landsförräderi, 4) spioneri, grovt spioneri, 5) röjande av statshemlighet, 6) olovlig underrättelseverksamhet, 7) brott som begåtts i terroristiskt syfte enligt 34 a kap. 1 § 1 mom. 2–7 punkten eller 2 mom. i strafflagen, 8) förberedelse till brott som begås i terroristiskt syfte, 9) ledande av terroristgrupp, 10) främjande av en terroristgrupps verksamhet, 11) meddelande av utbildning för ett terroristbrott, 12) deltagande i utbildning för ett terroristbrott, om gärningen är så allvarlig att den förutsätter fängelsestraff, 13) rekrytering för ett terroristbrott, 14) finansiering av terrorism, 15) finansiering av terroristgrupp, om gärningen är så allvarlig att den förutsätter fängelsestraff, 16) resa i syfte att begå ett terroristbrott, om gärningen är så allvarlig att den förutsätter fängelsestraff. Det är fråga om avslöjande av brott i fall som hör till skyddspolisen (RP 224/2010 rd, s. 95).

Det gemensamma draget för de befogenheter som skyddspolisen använder sig av (hemliga metoder för inhämtande av information) är att de har definierats utgående från person och brott. De får riktas in enbart på en sådan person eller användas för att inhämta information om verksamhet som bedrivs av enbart en sådan person som det finns grundad anledning att anta att i framtiden kommer att göra sig skyldig till, eller som redan har gjort sig skyldig till, ett brott av en viss allvarlighetsgrad, eller förberedelser till ett sådant brott.

Den person som är föremål för informationsinhämtningen ska kunna identifieras genom åtminstone sin roll eller uppgift, även om hens identitet ännu är okänd för polisen. Teleavlyssning eller teleövervakning kan riktas in även på en okänd person, till exempel på basis av en

IP-adress eller ett IMEI-nummer. Om det inte finns någon sådan här grund för brottsbekämpning i anslutning till en viss person är användningen av hemliga metoder för inhämtande av information enligt polislagen inte möjlig. Annat inhämtande av underrättelseuppgifter måste alltså basera sig på uppföljning av öppna källor, polisens så kallade allmänna övervakning och uppgifter som skyddspolisen får av andra myndigheter och privata sammanslutningar via sitt samarbetsnätverk.

Underrättelseverksamhet kännetecknas av att man inte alltid känner till en viss person, och det är ett viktigt mål för underrättelseinhämtningen att hitta personer vars verksamhet allvarligt hotar den nationella säkerheten. När det gäller grunderna för när befogenheter får användas bör befogenheterna för underrättelseinhämtning därför frigöras från den regel om att befogenheterna ska utgå från ett visst brott eller en viss person som gäller för närvarande.

Eftersom de särskilda förutsättningarna för användning av de nuvarande befogenheterna för informationsinhämtning har definierats utgående från brott och hur allvarliga de är, bör de särskilda förutsättningarna vad gäller befogenheterna för underrättelseinhämtning definieras utifrån hoten. Hemlig informationsinhämtning bör bli möjlig när det gäller sådan verksamhet som antingen direkt eller indirekt allvarligt hotar Finlands nationella säkerhet. Verksamhet som allvarligt hotar den nationella säkerheten kan vara sådan verksamhet som om den konkretiseras utgör ett brott, men som det ännu inte är möjligt att rikta någon konkret och specifik brottsmisstanke mot. Likaså kan det vara fråga om verksamhet som enligt finländsk lag inte är ett brott och som inte heller kan bli det.

Informationsinhämtningen bör också inbegripa kartläggning av externa hot mot Finland. Det kan då vara fråga om till exempel att följa utvecklingen i säkerhetsmiljön för att få fram en lägesbild vad gäller den nationella säkerheten. Framställningen ska också täcka in kontinuerlig informationsinhämtning om verksamhet som allvarligt hotar den nationella säkerheten. Informationsinhämtningen ska alltså inte vara tidsmässigt begränsad eftersom underrättelseverksamhet ofta behöver följas långsiktigt och systematiskt utan att den verksamhet som följs nödvändigtvis behöver vara direkt hotande medan uppföljningen pågår (Justitieministeriets betänkanden och utlåtanden 41/2016, s. 49, på finska). Verksamhet som allvarligt hotar den nationella säkerheten behandlas i detaljmotiveringen till 5 a kap. 3 § i förslaget till polislag.

Även om informationsinhämtningen är av långvarig art ska det för varje metod för underrättelseinhämtning föreskrivas särskilt om ett tillstånds eller besluts varaktighet. Varaktigheten ska kunna vara högst sex månader. Då ett tillstånd eller beslut har upphört att gälla ska ett nytt beslut fattas om användningen av underrättelseinhämtningsmetoden eller så ska användningen av metoden avslutas. Dessutom ska metodens nödvändighet och grunderna för den övervägas hela tiden medan den används, och användningen av metoden ska upphöra innan den tidsfrist som anges i beslutet har löpt ut ifall syftet med användningen har uppnåtts, eller om det inte längre finns förutsättningar för metoden.

Metoder för inhämtande av information ur telenät

Verksamhet som allvarligt hotar den nationella säkerheten är nästan undantagslöst förknippad med kommunikation. Eftersom sådan verksamhet till sin natur nästan alltid är organiserad, har de som deltar i den behov av att kommunicera med varandra. Detta gäller allt från terrorism, underrättelseinhämtning som riktas mot Finland av främmande makter, spridning av massförstörelsevapen och verksamhet som hotar kritisk infrastruktur i samhället till verksamhet som syftar till en våldsam omstörtning eller ändring av stats- och samhällsordningen. Beroende på arten av hotande verksamhet kan kommunikationen gälla till exempel uppdrag mellan dem som deltar i verksamheten, rapportering om hur olika uppgifter har utförts, planering av verksamheten, informationsinhämtning om mål för hotet, motivering och radikalisering av de del-

aktiga eller rekrytering av nya deltagare i verksamheten. Nuförtiden är kommunikationen i allmänhet elektronisk och den sker i datanät.

Informationsinhämtning som gäller elektronisk kommunikation mellan personer är i en nyckelposition när det behövs sådan information om hot som riktar sig mot den nationella säkerheten som gör det möjligt att få en tillräckligt klar lägesbild och att avvärja hot. Det är viktigt att få information om såväl innehållet i den elektroniska kommunikationen som andra uppgifter som ansluter sig till kommunikationen, såsom identifieringsuppgifter. På basis av innehållet i kommunikationen kan man skapa sig en mera konkret bild av vilken typ av verksamhet som hotar den nationella säkerheten samt av detaljerna i verksamheten. Identifieringsuppgifter kan vara nödvändiga för att identifiera de teleadresser eller den teleterminalutrustning som innehas av dem som deltar i verksamheten.

Sådana hemliga metoder för inhämtande av information ur telenät som ingriper i skyddet för hemligheten i fråga om förtroliga meddelanden som skyddspolisen har till sitt förfogande och som syftar till att förhindra eller avslöja brott är teleavlyssning enligt 5 §, inhämtande av information i stället för teleavlyssning enligt 6 §, teleövervakning enligt 8 § och teleövervakning med samtycke av den som innehar teleadress eller teleterminalutrustning enligt 9 § i polislagens 5 kap. I tvångsmedelslagen föreskrivs det om användningen av samma metoder för utredning av brott.

Vad som är gemensamt för de ovan nämnda hemliga metoderna för informationsinhämtning är att det krävs en noggrann identifiering av den teleadress eller teleterminalutrustning som metoden ska riktas mot för att sådana här metoder ska få användas. I fråga om teleavlyssning och inhämtande av information i stället för teleavlyssning finns det bestämmelser om kravet på identifiering i 5 kap. 7 § 3 mom. 5 punkten i polislagen. Enligt bestämmelsen ska den teleadress eller teleterminalutrustning som åtgärden riktas mot nämnas i ett yrkande eller beslut om användning av en metod för inhämtande av information. Enligt 5 kap. 5 § 2 mom. och 6 § 1 mom. i polislagen får teleavlyssning och inhämtande av information i stället för teleavlyssning riktas enbart mot en sådan teleadress eller teleterminalutrustning som ägs eller som sannolikt används av en person som med fog kan antas göra sig skyldig till något av de allvarliga brott som nämns särskilt i 5 § 2 mom.

I fråga om teleövervakning liksom teleövervakning med samtycke av den som innehar teleadress eller teleterminalutrustning finns det i 5 kap. 10 § 6 mom. 6 punkten i polislagen en bestämmelse om att den teleadress eller teleterminalutrustning som åtgärden riktas mot ska nämnas i ett yrkande eller beslut om användning av en metod för inhämtande av information. Enligt 5 kap. 8 § 2 mom. i polislagen får teleövervakning riktas enbart mot en teleadress eller teleterminalutrustning som ägs eller sannolikt används av en person som med fog kan antas göra sig skyldig till ett brott av en viss allvarlighetsgrad eller något av de brott som nämns särskilt i bestämmelsen. Så kallad teleövervakning med samtycke får enligt polislagens 9 § riktas enbart mot en teleadress eller teleterminalutrustning som innehas av den som gett sitt samtycke.

Det att den teleadress eller teleterminalutrustning som en åtgärd ska riktas mot ska nämnas i ett yrkande om tillstånd att använda en metod för inhämtande av information ur telenät och i ett beslut som meddelas med anledning av ett sådant yrkande betyder inte att polisen måste känna till namnet på den som äger eller som annars använder teleadressen eller teleterminalutrustningen. Hen kan också vara en person som ännu är okänd för polisen, men som med fog kan misstänkas till exempel vara delaktig i en straffbar gärning. Personen kan då i ett yrkande som gäller användning av en metod för inhämtande av information ur telenät och i ett domstolsbeslut som meddelas med anledning av yrkandet individualiseras med hjälp av en teleadress eller teleterminalutrustning som hen innehar eller annars kan antas använda och med hjälp av hens delaktighet (RP 224/2010 rd, s. 98).

Teleavlyssning och teleövervakning får riktas enbart mot en teleadress eller teleterminalutrustning som med en viss säkerhet innehas eller används av en viss person. I beslutet om teleavlyssning eller teleövervakning ska också personen i fråga nämnas, men hen får vara okänd. Ingendera av dessa informationsinhämtningsmetoder får riktas mot enbart en person, utan identifiering av en teleadress eller teleterminalutrustning. Ett särskilt tillstånd ska sökas för varje teleadress och teleterminalutrustning. Detta är problematiskt i och med att man, när det gäller professionella och organiserade personer som utgör hot, på grund av verksamhetens särdrag måste kunna agera utifrån vidare kriterier för inriktningen av det hemliga inhämtandet av information.

Det är mycket enkelt att skaffa sig ett förhandsbetalt (prepaid) abonnemang och andra anonyma abonnemang, och de har i takt med den tekniska utvecklingen blivit förmånliga att både skaffa sig och använda. En person kan förfoga över flera tiotal anonyma abonnemang och teleterminalutrustningar (mobiltelefoner). Detta gör att teleavlyssning och teleövervakning i många fall blir mycket arbetskrävande och att effekten av åtgärderna som hemliga informationsinhämtningsmetoder minskar. Dessutom ger det upphov till onödiga personalkostnader för förundersökningsmyndigheterna, domstolsväsendet och teleföretagen. Det är skäl att utvidga bestämmelserna om sådan inriktning av teleavlyssning och teleövervakning som görs i syfte att inhämta underrättelser så att de också gäller personer. På det viset kommer teleavlyssning att gälla kommunikation som kommer från eller som är ämnad för bara en viss person, och om man hittar nya teleabonnemang och teleterminalutrustningar i personens innehav behöver man inte ansöka om flera nya tillstånd under den tid det personspecifika tillståndet gäller. På så sätt behövs det inte flera tillståndsbeslut som gäller samma person, vilket bidrar till att minska arbetsbördan för de aktörer som är involverade i tillståndsprocessen. Till exempel terroristceller försöker skydda sin verksamhet och sina kontakter genom att använda flera olika identiteter och vilseleda underrättelsemyndigheterna bland annat genom att använda flera olika telefonabonnemang och telefoner.

Tekniska villkor för metoder för inhämtande av information ur telenät

Den ovan beskrivna regleringen av metoderna för inhämtande av information ur telenät påverkar hur teleavlyssningen och teleövervakningen utförs rent tekniskt. Teleavlyssning och teleövervakning utförs i så nära anslutning som möjligt till den teleadress eller teleterminalutrustning som är föremål för informationsinhämtningen, det vill säga på ett ställe där det inte rör sig någon annan kommunikation än den som går ut från eller kommer in till den adress eller terminalutrustning som är föremål för informationsinhämtningen. Nätverkstopologiskt, det vill säga med avseende på den logiska uppbyggnaden av kommunikationsnätet, sker teleavlyssning och teleövervakning på kanten av kommunikationsnätet.

Metoder för inhämtande av information ur telenät kan inte användas om polisen inte känner till de enskilda teleadresser och teleterminalutrustningar som används i kommunikationen inom den verksamhet som är föremål för polisens informationsinhämtning. Dessa metoder kan då inte heller användas i fall där det i sig finns uppgifter eller misstankar om ett sådant brott som utgör grund för teleavlyssning eller teleövervakning, eller om fakta som gäller ett sådant brott. Metoderna för inhämtande av information ur telenät möjliggör inte informationsinhämtning om vilka medier eller kanaler som används i den verksamhet som är föremål för informationsinhämtningen eftersom existensen av uppgifter om medier eller kanaler är en lagstadgad förutsättning för användningen av dessa metoder och likaså en förutsättning för att de ska kunna genomföras tekniskt.

Om polisen känner till en person som med fog kan antas göra sig skyldig till ett sådant brott som utgör grund för teleavlyssning eller teleövervakning, men inte enskilda teleadresser eller teleterminalutrustningar som används av personen i fråga, kan identifieringsuppgifter för tele-

adresser eller teleterminalutrustning till exempel inhämtas med stöd av de befogenheter som det föreskrivs om i 5 kap. 25 § i polislagen. För att förhindra brott får polisen enligt den paragrafen med en teknisk anordning inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning, när det är fråga om brott för vilket det föreskrivna strängaste straffet är fängelse i minst ett år. Den tekniska anordning som används i verksamheten ska vara sådan att den inte kan användas för något annat ändamål än för identifiering av teleadresser eller teleterminalutrustningar. Inhämtning av identifieringsuppgifter för teleadresser eller teleterminalutrustningar med stöd av de befogenheter som avses i 5 kap. 25 § i polislagen gör det möjligt att i ett senare skede rikta in teleavlyssning eller teleövervakning mot en adress eller terminalutrustning då de förutsättningar som föreskrivits för dessa informationsinhämtningsmetoder uppfylls.

På det sätt som konstateras i regeringens proposition RP 266/2004 rd (s. 37) inhämtas identifieringsuppgifter för teleadresser eller teleterminalutrustning med hjälp av ett slags falsk basstation utan att man behöver koppla in privata teleföretag i myndigheternas informationsinhämtning. Den tekniska anordningen måste användas i fysisk närhet till den person som använder den teleadress eller teleterminalutrustning som man vill få fram identifieringsuppgifter för. För att en befogenhet ska kunna användas krävs det alltså i praktiken att polisen känner till såväl den person som är föremål för åtgärden som hens uppehållsplats. Personens uppehållsplats måste naturligtvis vara i Finland vid den tidpunkt då anordningen används.

Polisens nuvarande metoder för inhämtande av information ur telenät lämpar sig för informationsinhämtning endast då det är fråga om sådana brott som man redan med viss säkerhet känner till, som uppfyller vissa brottsrekvisit och som är under planering eller antas ha blivit begångna, och där polisen känner till vilka personer som är delaktiga och de individuella teleadresser och teleterminalutrustningar som personerna använder då informationsinhämtningen inleds. Med avseende på underrättelseverksamhet lämpar sig inte de hemliga metoder för inhämtande av information ur telenät som anges i polislagen för upptäckande och identifiering av hot. Detta beror på förutsättningarna för inriktningen av hemliga metoder för inhämtande av information ur telenät samt de särskilda förutsättningarna för användningen av informationsinhämtningsmetoderna.

Teleavlyssning har sina brister när det gäller upptäckt och identifiering av hot i det allmänna kommunikationsnätet. Med tanke på det har det ingen avgörande betydelse om till exempel grunden för teleavlyssning och teleövervakning på samma sätt som nu är att förhindra brott eller om dessa informationsinhämtningsmetoder också kunde användas som metoder för underrättelseinhämtning för att få fram information om verksamhet som hotar den nationella säkerheten. Den uttryckliga förutsättningen för att metoderna ska få användas även med underrättelseinhämtning som grund är kännedomen om ett hot, personerna bakom hotet och de konkreta kommunikationsmedier som dessa personer använder vid den tidpunkt då man inleder teleavlyssningen eller teleövervakningen. Bestämmelser om teleavlyssning och teleövervakning som grundar sig på underrättelseinhämtning ökar följaktligen inte i betydande grad det finländska samhällets förmåga att i det allmänna kommunikationsnätet upptäcka och identifiera okända hot som riktar sig mot dess viktigaste säkerhetsintressen och de personer som ligger bakom hoten. En separat aspekt är att man kan beräkna att bestämmelser om teleavlyssning och teleövervakning som grundar sig på underrättelseinhämtning på ett betydelsefullt sätt kan förbättra tillgången till information om sådan verksamhet som allvarligt hotar den nationella säkerheten där det inte är fråga om ett brott eller där man inte har nått nivån för en konkret och specifik brottsmisstanke. Till denna del är det fråga om en utvidgning av det materiella tillämpningsområdet för metoderna för inhämtande av information ur telenät, som ändå inte kommer att förändra metodernas grundkaraktär. Samma observation gäller i fråga om ett utvidgade av det materiella tillämpningsområdet för dessa metoder där man kriminaliserar sådana verksamhetsformer som allvarligt hotar den nationella säkerheten som för närvarande inte

är straffbara. En utvidgning av de brott som utgör särskilda förutsättningar för användningen av dessa metoder kommer inte att förändra metodernas grundkaraktär.

Ett allt vanligare drag hos de allvarliga säkerhetshot som omfattas av skyddspolisens ansvarsområde är att de personer som är delaktiga befinner sig utanför Finlands gränser, vilket betyder att den elektroniska kommunikationen mellan dem överskrider gränserna mellan olika stater. Bristerna i de metoder för inhämtande av information ur telenät som det föreskrivs om i polislagens 5 kap. accentueras ofta då man behöver få information om kommunikation som sker mellan Finland och något annat land. Det är ofta fråga om situationer där den kommunikationspart som befinner sig i utlandet med en viss exakthet är känd, till exempel till följd av internationellt informationsutbyte mellan underrättelse- och säkerhetstjänster, medan den part som befinner sig i Finland är okänd. Det kan till exempel vara fråga om situationer där man vet eller misstänker att ett terroristnätverk i utlandet radikaliserar eller värvar personer i Finland eller styr medlemmar som sänts hit eller som annars uppehåller sig här, eller där man har fått kännedom om att en främmande stats underrättelsetjänst har sänt underrättelseofficerare till Finland under täckmantel. Om man inte känner till de personer som deltar i verksamheten i Finland och de kommunikationsmedier som de använder, kan man inte rikta in informationsinhämtning ur telenät mot gränsöverskridande kommunikation även om man kände till den kommunikationspart som befinner sig i utlandet. De nuvarande metoderna för inhämtande av information ur telenät kan med andra ord inte användas för att upptäcka eller identifiera personer i Finland som är delaktiga i gränsöverskridande hot mot den nationella säkerheten, även om en upptäckt och identifiering av dem är en förutsättning för en mera exakt informationsinhämtning om hot och i sista hand för avvärjning av hot. Detta är en betydande brist i en situation där Finlands säkerhetsmiljö har försämrats på ett avgörande sätt inom så gott som alla sektorer och sannolikt också kommer att fortsätta att försämras.

Finlands säkerhetsmiljö har utvecklats och kommer uppenbarligen att fortsätta att utvecklas i en riktning där det blir allt svårare att i tid upptäcka och identifiera allvarliga hot mot den nationella säkerheten. Den bakomliggande och allt mera skiftande hotmiljön har behandlats i bland annat statsrådets redogörelse för den inre säkerheten (SRR 5/2016 rd) och statsrådets utrikes- och säkerhetspolitiska redogörelse (SRR 6/2016 rd). En tidig upptäckt och identifiering av hot och förmåga att kunna förutse förändringar i hotmiljön har samtidigt blivit ännu viktigare än förut i och med att teknikens utveckling har gjort det möjligt att utföra handlingar som äventyrar den nationella säkerheten med kortare förberedelsetid och allvarligare följder än förut.

Det är tekniskt möjligt att ordna det så att hot mot den nationella säkerheten kan upptäckas och identifieras i den elektroniska kommunikationsmiljön. För att förmågan att upptäcka och identifiera hot ska utvecklas krävs det emellertid en lösning som till sina grundläggande egenskaper avviker från polisens nuvarande metoder för inhämtande av information ur telenät, som innebär att informationsinhämtningen sker med hjälp av ett system som filtrerar strömmen av meddelande- och datatrafik. Nätverkstopologiskt innebär detta att informationsinhämtningen sker i mitten av kommunikationsnätet, vilket är tvärtemot jämfört med när man använder de metoder för inhämtande av information ur telenät som det föreskrivs om i den gällande lagstiftningen. Genom att placera det filter som används vid informationsinhämtningen i mitten av kommunikationsnätet strävar man efter att säkerställa att det med så stor sannolikhet som möjligt strömmar sådan meddelande- eller datatrafik genom filtersystemet som kan antas ha att göra med verksamhet som allvarligt hotar den nationella säkerheten. Vid filtreringen skiljs sådan kommunikation som är väsentlig med tanke på hot ur från annan datatrafik med hjälp av vissa förinställda kriterier eller filtreringsparametrar. Som filtreringsparametrar kan man använda till exempel sådana uttryck som används i kommunikationen, särskilda kommunikationsvanor, IP-adressrymder eller uppgifter om tiden och platsen för kommunikationen som

man vet eller förmodar har koppling till den verksamhet som är föremål för informationsinhämtningen.

Ett tillvägagångssätt som baserar sig på filtrering torde till viss del kunna jämföras med sådan profilering som används i annan verksamhet som bedrivs av säkerhetsmyndigheterna med vars hjälp man i en större målgrupp söker avvikelser som är väsentliga med tanke på säkerheten. Funktionsmässigt är filtrering av meddelandetrafiken jämförbar med till exempel sådan gräns- och tullövervakning som grundar sig på profilering och riskbedömning. Inom gräns- och tullövervakningen kan en del av de personer som passerar gränsen väljas ut för närmare granskning på basis av att de uppfyller vissa sållningsparametrar som bestämts i förväg, till exempel vad gäller resesättet. Förutom på allmänna uppgifter om mänskligt beteende eller verksamhetssätt kan filtreringen av meddelandetrafiken emellertid också grunda sig på konkreta uppgifter som beskriver det hot som är föremål för informationsinhämtningen. Som ett exempel på sådana uppgifter kan nämnas uppgifter om att man i den kommunikation som ansluter sig till det hot som är föremål för informationsinhämtningen använder sådan programkod som enbart används av personer som deltar i hotkommunikationen.

Av avsnitt 2.3 i propositionen framgår det att man i majoriteten av jämförelseländerna använder eller planerar att införa informationsinhämtningsmetoder som grundar sig på filtrering av meddelande- och datatrafiken. Dessa metoder kan, trots deras inbördes skillnader, gå under den gemensamma benämningen underrättelseinhämtning som avser datatrafik. Syftet med den underrättelseinhämtning som avser datatrafik som man använder sig av eller planerar i jämförelseländerna är att upptäcka hot mot den nationella säkerheten, identifiera de personer som ligger bakom dem, identifiera teleadresser och teleterminalutrustning som används i den hotfulla verksamheten i syfte att möjliggöra teleavlyssning och teleövervakning samt att inhämta närmare information om hoten.

I jämförelseländerna används underrättelseinhämtning som avser datatrafik i huvudsak som en underrättelseinhämtningsmetod även om den i vissa länder också kan användas för bekämpning av allvarliga brott. Syftet med underrättelseinhämtning är att upptäcka och identifiera hot mot de viktigaste nationella säkerhetsintressena och att dela analyserad information om hoten med de aktörer som behöver denna information. Syftet är alltså inte att man med tanke på en framtida straffprocess ska skaffa fram information om en person som redan är känd och som med fog kan antas göra sig skyldig till eller misstänkas ha gjort sig skyldig till ett brott av en viss allvarlighetsgrad. Underrättelseinhämtning som avser datatrafik skiljer sig från polisens traditionella metoder för inhämtande av information ur telenät och andra informationsinhämtningsmetoder och även från de flesta av de metoder som används av underrättelsetjänsterna just av den orsaken att den på grund av sina tekniska särdrag gör det möjligt att upptäcka och identifiera hot som tidigare varit okända.

Med hjälp av underrättelseinhämtning som avser datatrafik inhämtas det i jämförelseländerna inte bara sådan information som betjänar statsledningens utrikes- och säkerhetspolitiska beslutsfattande utan också sådan information som behövs för att avvärja hot i ett så tidigt skede som möjligt. För att hot ska kunna avvärjas kan information som inhämtats genom underrättelseinhämtning som avser datatrafik i allmänhet under vissa förutsättningar överlämnas till polisen, som på basis av informationen kan ingripa i till exempel förberedelser för terroristisk verksamhet. Beroende på landet och genom olika förfaranden kan information överlämnas även till andra förvaltningsmyndigheter, såsom de myndigheter vars ansvarsområde omfattar inresor och övervakning av inresor, och i så fall kan hotfull verksamhet avvärjas med administrativa åtgärder redan vid den yttre gränsen. Överlämnandet av information till polisen och andra myndigheter är i allmänhet ändå begränsat på något sätt, eftersom det inte har ansetts vara lämpligt att en metod såsom underrättelseinhämtning som avser datatrafik, som är synnerligen effektiv och som till sin karaktär skiljer sig från andra informationsinhämtningsme-

toder, ska kunna användas för att inhämta information om vilka brott, hot eller risker som helst.

De filtreringsparametrar som används inom underrättelseinhämtning som avser datatrafik och som kan benämnas sökbegrepp kan filtrera innehållet eller andra uppgifter i den meddelande- och datatrafik som strömmar igenom underrättelsesystemet. Andra uppgifter är till exempel sådana uppgifter som behövs för att styra enskilda meddelanden i strömmen av datatrafik från avsändaren till mottagaren samt uppgifter om tid och plats för kommunikationen.

Effektiviteten i sådan här underrättelseinhämtning, men även dess konsekvenser för de grundläggande rättigheterna, beror på om man som sökbegrepp använder uppgifter som beskriver innehållet i ett meddelande eller enbart andra uppgifter i anslutning till kommunikationen. Effektiviteten blir större om man kan använda uppgifter som beskriver innehållet i ett meddelande som sökbegrepp. I så fall behöver underrättelsemyndigheten inte i förväg känna till exempelvis i vilken adressrymd parterna skickar sina meddelanden, utan i alla meddelanden som ingår i strömmen av datatrafik kan det sökas till exempel sådana ovanliga namn eller kodade uttryck som man vet eller kan anta att används i samband med till exempel terroristisk verksamhet eller spionage som bedrivs av en främmande stat som ska utredas. Sökbegrepp som beskriver innehållet i ett meddelande behövs alltså framför allt då man inte känner till eller då man bara har mycket allmän kunskap om vilka kommunikationskanaler som används i den verksamhet som är föremål för informationsinhämtningen. Å andra sidan utgör användningen av sökbegrepp som gäller innehållet ett större ingripande i förtrolig kommunikation än andra sökbegrepp, i och med att det förutsätter att all kommunikation som strömmar igenom, det vill säga även kommunikationen mellan alla personer som med avseende på hotet är utomstående, öppnas och att sökbegreppen jämförs med innehållet i meddelandena.

Användningen av sökbegrepp som beskriver innehållet i kommunikationen är tillåten eller planeras bli tillåten i alla de jämförelseländer som har infört bestämmelser om underrättelseinhämtning som avser datatrafik eller som bereder sådan lagstiftning. Användningen av sökbegrepp som gäller innehållet har emellertid begränsats antingen i lag eller i motiven till lagarna så att sökbegreppen enbart får vara andra uttryck än sådana vanliga uttryck som ingår i allmänspråket. Tillåtna sökbegrepp kan alltså vara närmast sådana ovanliga personnamn och uttryck som inte är allmänt kända eller använda och som man på så sätt inte kan anta förekommer i kommunikationen mellan utomstående.

I fråga om de sökbegrepp som gäller innehållet begränsas användbarheten och effektiviteten av att krypteringsteknikerna har utvecklats och att det har blivit vanligare att sådana används. Andra uppgifter som är kopplade till kommunikationen kan inte döljas på samma sätt som meddelandenas innehåll eftersom de behövs för att styra meddelandena från avsändaren till mottagaren i kommunikationsnätet. Uppgifterna för styrning och förmedling av kommunikationen har alltså stor betydelse som sökbegrepp vid underrättelseinhämtning som avser datatrafik. I betänkandet från arbetsgruppen för en informationsanskaffningslag är bedömningen (s. 72, på finska) att man genom underrättelseinhämtning som avser datatrafik trots kryptering kan få fram information som är viktig med tanke på den nationella säkerheten till exempel med hjälp av identifieringsuppgifter.

Underrättelseinhämtning som avser datatrafik kan användas för att upptäcka, identifiera och utreda sådana hot mot det land som bedriver underrättelseinhämtningen som kommer både utifrån och inifrån själva landet. I jämförelsestaterna används sådan här underrättelseinhämtning enbart för att upptäcka, identifiera och utreda externa hot, det vill säga som en metod för underrättelseinhämtning som avser utländska förhållanden. Därför har underrättelseinhämtning som avser datatrafik i jämförelsestaterna ordnats så att den gäller den gränsöverskridande meddelande- och datatrafiken i den stat som bedriver underrättelseinhämtningen.

Av jämförelsestaternas lagstiftning och motivdokumenten till lagstiftningen kan man sluta sig till att underrättelseinhämtning som avser datatrafik i dessa stater har ordnats eller kommer att ordnas som en verksamhet som sker i flera steg. Trots skillnader i de olika ländernas lagstiftning kan verksamheten generellt beskrivas så att man först väljer ut de delar av de gränsöverskridande datatrafikförbindelserna genom vilka det kan antas strömma sådan kommunikation eller annan datatrafik som är kopplad till den verksamhet som är föremål för underrättelseinhämtningen. Den kommunikation eller annan datatrafik som löper genom de utvalda datatrafikförbindelserna styrs antingen över så att den går igenom det datasystem som används vid underrättelseinhämtningen eller så skapas det en kopia av informationen som kan sparas. I det förstnämnda fallet jämför datasystemet i realtid den kommunikation och datatrafik som strömmar igenom det med de förhandsinställda sökbegreppen. Kommunikation och annan datatrafik som motsvarar sökbegreppen styrs över till en analysdatabas för fortsatt behandling. Annan kommunikation och datatrafik än sådan som motsvarar sökbegreppen går igenom underrättelsesystemet och kan inte återfås senare för granskning. I det senare nämnda fallet används inte sökbegreppen i realtid utan den trafik som kopierats styrs i sin helhet över till en analysdatabas, där man senare kan utföra sökningar i materialet.

I avsnitt 2.4 och 2.5 i propositionen beskrivs den rättspraxis hos Europadomstolen och EU-domstolen som är relevant med tanke på hur underrättelseinhämtning som avser datatrafik ska ordnas. Av beskrivningen framgår att Europadomstolen har ansett att underrättelseinhämtning som avser datatrafik som har ordnats med vissa förhållandevis stränga villkor är förenlig med artikel 8 i Europakonventionen.

Då godtagbarheten av underrättelseinhämtning som avser datatrafik ska bedömas ur Europakonventionens och EU-rättens perspektiv är det med avseende på den internationella domstolspraxisen av särskild betydelse att den nationella lagstiftningen överensstämmer med proportionalitetsprincipen. Europadomstolens uppfattning av vilka minimikrav som följer av proportionalitetsprincipen framgår av det test som domstolen skapade i sina avgöranden i fallen Huvig mot Frankrike 24.4.1990 och Kruslin mot Frankrike 24.4.1990, och som den i sina senare avgöranden upprepade gånger har tillämpat och i viss mån även vidareutvecklat. Också i EU-domstolens avgörande i fallet Digital Rights Ireland var det i mångt och mycket fråga om en tillämpning av det ovannämnda så kallade Huvig/Kruslin-testet. Enligt detta test ska nationell lagstiftning som tillåter ingripanden i kommunikationshemligheten innehålla: 1) en definition av de personer vars kommunikationshemlighet man vill ingripa i, 2) en definition av vilka gärningar eller hot som berättigar till ett ingripande i kommunikationshemligheten, 3) bestämmelser om hur man beslutar om ett ingripande, 4) bestämmelser om hur uppgifter får behandlas, användas och förvaras, 5) bestämmelser om hur länge ett ingripande i kommunikationshemligheten får pågå och om förvaringstiderna för uppgifter som samlats in med hjälp av åtgärderna, 6) bestämmelser om säkerhetsåtgärder då uppgifter överlämnas åt andra samt 7) bestämmelser om de förfaranden som ska iakttas då uppgifter avlägsnas eller utplånas.

I betänkandet från arbetsgruppen för en informationsanskaffningslag gjordes det en preliminär bedömning av hurdan lagstiftning om underrättelseinhämtning som avser datatrafik som skulle kunna stiftas i Finland så att bestämmelserna uppfyller de krav som följer av de ovannämnda kriterierna som konkretiserar proportionalitetsprincipen och även mera generellt av den internationella rättspraxisen.

De internationella människorättsavtal som är förpliktande för Finland tillåter på vissa villkor underrättelseinhämtning som riktar sig mot såväl intern som gränsöverskridande datatrafik. Eftersom de allvarligaste hoten mot Finlands nationella säkerhet i första hand är externa, ansluter sig Finlands behov uttryckligen till underrättelseinhämtning om gränsöverskridande datatrafik. De hot som informationsinhämtningen inom den underrättelseinhämtning som avser datatrafik skulle få gälla måste å sin sida definieras i lag på ett så klart och kortfattat sätt som

möjligt. Hoten måste vara tillräckligt allvarliga och rikta sig mot viktiga säkerhetsintressen med tanke på den nationella säkerheten. Vad som är klart är att underrättelseinhämtning som avser datatrafik inte kan vara en metod för att undersöka sådan nätkriminalitet eller annan masskriminalitet som bör betraktas som vanlig. Arbetsgruppen för en informationsanskaffningslag går emellertid längre än så och rekommenderar att man när man överväger bestämmelser om underrättelseinhämtning som avser datatrafik ska utgå från att det inte ska vara tillåtet att använda metoden som brottsutredningsmetod (s. 62–63 i betänkandet, på finska).

Underrättelseinhämtning som avser datatrafik som överskrider Finlands gränser bör genomföras på ett sådant sätt att man i flödet av datatrafik så effektivt som möjligt kan sålla ut den trafik som är relevant med tanke på de allvarliga hot som ligger till grund för verksamheten och förhindra att trafik som inte hör till uppdragen blir föremål för analys. Vid sållningen ska man därför använda tillräckligt exakta och på förhand bestämda sökbegrepp eller sådana verbala beskrivningar av verksamhet som äventyrar den nationella säkerheten som så konkret som möjligt beskriver föremålet för informationsinhämtningen. Objekt för beskrivningen blir sådana kommunikationsmodeller och andra verksamhetsmodeller som man vet eller kan anta att ansluter sig till verksamhet som äventyrar den nationella säkerheten. En tillståndsmyndighet som är separat från underrättelsemyndigheten ska godkänna sökbegreppen och de muntliga beskrivningarna, och användningen av dem vid underrättelseinhämtning ska dokumenteras ingående med tanke på efterhandstillsyn. Arbetsgruppen för en informationsanskaffningslag föreslår att en domstol ska vara tillståndsmyndighet, och när det gäller efterhandstillsynen föreslår arbetsgruppen att man överväger att inrätta ett nytt oberoende organ för laglighetsövervakning (s. 67–69 i betänkandet, på finska).

Arbetsgruppen rekommenderar att de sökbegrepp som ska vara tillåtna vid underrättelseinhämtning som avser datatrafik ska begränsas så att enbart identifieringsuppgifter får användas. Som exempel på sådana sökbegrepp nämns identifieringsuppgifter för adaptrar och nätadresser samt uppgifter som beskriver tiden och platsen för kommunikationen. Följaktligen intog arbetsgruppen en ståndpunkt som avvek från och som var strängare än lagstiftningen i de jämförelseländer som behandlats ovan när det gäller användningen av sökbegrepp som gäller innehållet. Ifall syftet med underrättelseinhämtning som avser datatrafik är att upptäcka spionage i datanät som genomförs med hjälp av skadeprogram skulle emellertid även sökbegrepp som beskriver innehållet i meddelanden kunna användas i undantagsfall. Det sökbegrepp som beskriver innehållet skulle i så fall vara den tekniska identifikationen för skadeprogrammet (s. 64 i betänkandet, på finska).

Det är motiverat att den filtrering av meddelande- och datatrafiken som sker med hjälp av sökbegrepp utförs maskinellt. De meddelanden som har separerats från den övriga datatrafiken med hjälp av sökbegrepp och som man i princip kan anta är relevanta för utredningen av det hot som är föremål för informationsinhämtningen ska få bli föremål för manuell behandling, och då får också deras innehåll klarläggas. De meddelanden som på basis av klarläggandet av innehållet konstateras vara kopplade till det hot som är föremål för underrättelseinhämtningen ska också få sparas. Också sådana meddelanden ska få sparas som ansluter sig till något annat hot mot den nationella säkerheten som nämns i lagen än det som tillståndet för underrättelseinhämtning som avser datatrafik har beviljats för. Däremot ska överflödig information som inte har med nationell säkerhet att göra omedelbart förstöras då det har konstaterats att så är fallet. Om syftet med underrättelseinhämtning som avser datatrafik är att inhämta information om externa hot i den datatrafik som överskrider Finlands gräns är det motiverat att sådan datatrafik mellan parter som befinner sig i Finland som av tekniska skäl fångas in vid underrättelseinhämtningen förstörs (s. 68 i betänkandet, på finska).

När det mera allmänt gäller behandlingen av uppgifter som inhämtats genom underrättelseinhämtning som avser datatrafik konstateras det i betänkandet att Europadomstolens avgörande-

praxis förutsätter att det införs tillräckligt exakta bestämmelser i lag om granskning och användning av uppgifter, om uppgifternas förvaringstider och om utlämnande och utplåning av uppgifter. Till exempel när det gäller utlämnande av uppgifter till en utländsk myndighet rekommenderas det att man har som utgångspunkt att utlämnandet av uppgifterna ska främja den nationella säkerheten och att det inte äventyrar Finlands intressen, inbegripet nationalekonomiska intressen.

Arbetsgruppen för en informationsanskaffningslag konstaterar att om det införs bestämmelser om underrättelseinhämtning som avser datatrafik på det sätt som den föreslår leder det inte till sådan omfattande, ospecificerad, långvarig och obegränsad registrering av identifieringsuppgifter som de internationella domstolarna i sin rättspraxis har ansett strida mot proportionalitetsprincipen. Detta konstaterande gäller uttryckligen identifieringsuppgifter, men det kan naturligtvis även gälla uppgifter om innehållet i kommunikation.

I beslutet om att tillsätta den arbetsgrupp som tillsattes för beredningen av denna regeringsproposition konstateras det att man i lagberedningsprojektet ska beakta betänkandet från arbetsgruppen för en informationsanskaffningslag och den respons som gavs i utlåtandena om betänkandet. Åläggandet att beakta betänkandet gäller även hur man ordnar den underrättelseinhämtning som avser datatrafik.

Inhämtning av information om datanätshot

De aktörer som hotar den nationella säkerheten kan emellertid använda elektroniska kommunikationsnät inte bara till kommunikation i anslutning till hoten utan också till att verkställa hot. Cybergärningar som utförts via kommunikationsnät, såsom cyberspionage, cyberterrorism, cyberaktioner som inbegriper påtryckningar och cybersabotage som riktar sig mot livsviktiga funktioner i en stat, kan i värsta fall äventyra statens livsduglighet eller centrala säkerhetsintressen. Förutom stater kan också privata företag eller sammanslutningar bli måltavlor för cybergärningar och då kan gärningarna äventyra till exempel hemligstämplad information om produktutveckling.

En förutsättning för att man ska kunna förhindra cyberhot eller åtminstone begränsa de skadliga konsekvenserna av dem är att de upptäcks i ett tillräckligt tidigt skede. Polisens metoder för inhämtande av information ur telenät och andra informationsinhämtningsmetoder är mycket dåligt lämpade för upptäckt av gärningar som utförts i cybermiljöer. Orsaken till att de är dåligt lämpade är å ena sidan de tidigare behandlade särdragen i metoderna för inhämtande av information ur telenät, som i detta sammanhang kan generaliseras till att gälla alla av polisens hemliga metoder för inhämtande av information. Förutsättningen för att polisens hemliga metoder för inhämtande av information ska få användas är att objektet, det vill säga en teleadress eller teleterminalutrustning när det gäller metoder för inhämtande av information ur telenät och en person när det gäller till exempel metoder av observationskaraktär, är känt i det ögonblick då informationsinhämtningen inleds.

Å andra sidan beror det att polisens metoder för informationsinhämtning är dåligt lämpade för upptäckt av cyberhot också på cyberhotens särdrag. De cybergärningar som riktar sig mot Finland och dess nationella säkerhet verkställs i allmänhet utanför landets gränser och de kräver ingen form av fysisk närvaro i landet. De finländska myndigheterna kan följaktligen inte ens i princip få vetskap om gärningarna före den stund då den attackvektor som används för gärningen, i regel ett tekniskt skadeprogram, överskrider Finlands gräns i kommunikationsnätet. Tidsspannet mellan den tidpunkten och de skadliga konsekvenserna av gärningen kan vara mycket kort. Eftersom det är fråga om gärningar som i sin helhet utförs i elektroniska kommunikationsnät kan de dessutom verkställas med hjälp av nästan vilken teleadress eller teleterminalutrustning som helst. I fråga om cybergärningar behöver man inte använda, och an-

vänds i allmänhet inte heller, en teleadress eller teleterminalutrustning som finns i det land eller som annars pekar mot det land som ligger bakom gärningen eller där gärningspersonen annars befinner sig. Cyberverksamhetsmiljön erbjuder utmärkta möjligheter till vilseledning i fråga om objektet för gärningen och till att dölja spåren efter gärningspersonen. Utmärkande drag för sådana gärningar som allvarligt hotar den nationella säkerheten och som utförs i cyberverksamhetsmiljön är sammanfattningsvis låga kostnader för att utföra gärningarna, möjlighet att använda samma vektorer upprepade gånger och mot flera måltavlor, svårigheten och de höga kostnaderna i fråga om att skydda sig mot gärningarna och den obetydliga risken att bli fast.

Möjligheterna att upptäcka och förhindra cybergärningar som äventyrar den nationella säkerheten grundar sig för närvarande i huvudsak på befogenheterna i 272 § i lagen om tjänster inom elektronisk kommunikation. Bestämmelsen ger företag, sammanslutningar och myndigheter som använder sig av elektroniska kommunikationstjänster rätt att i syfte att sörja för informationssäkerheten analysera innehållet i meddelanden som kommer in i eller lämnar deras nät för att bland annat upptäcka, förhindra och utreda störningar som kan ha en menlig inverkan och göra störningarna föremål för förundersökning. Bestämmelsen tillåter också automatiskt förhindrande eller automatisk begränsning av förmedling och mottagande av meddelanden, automatiskt avlägsnande av sådana skadliga datorprogram ur meddelandena som kan äventyra informationssäkerheten och andra åtgärder av teknisk natur som är jämförbara med detta.

Skadliga program och kommandon identifieras först genom en automatisk innehållslig analys på basis av kriterier som fastställts i förväg. Om det är uppenbart att ett meddelande som framträtt i den automatiska analysen innehåller ett skadeprogram och att informationssäkerheten inte kan säkerställas med automatiska åtgärder, tillåter 272 § i lagen om tjänster inom elektronisk kommunikation att ett företag, en sammanslutning eller en myndighet behandlar innehållet i meddelandet manuellt.

Aktörer som är särskilt viktiga med tanke på den nationella säkerheten använder inte nödvändigtvis själva enbart de verksamhetsrättigheter som avses i 272 § i lagen om tjänster inom elektronisk kommunikation, utan deras datanät kan även skyddas av det så kallade HAVARO-systemet. HAVARO är ett system för att upptäcka och varna för kränkningar av informationssäkerheten som Kommunikationsverkets Cybersäkerhetscenter erbjuder företag som är kritiska med tanke på försörjningsberedskapen och aktörer inom statsförvaltningen. Verksamheten med systemet grundar sig på 272 § i lagen om tjänster inom elektronisk kommunikation. Ett syfte med HAVARO är att med hjälp av olika identifieringsuppgifter identifiera skadlig nättrafik och avancerade nätattacker som äventyrar informationssäkerheten (Advanced Persistent Threat, allmänt kallat APT). Ett annat syfte är att hjälpa till med att få fram en bättre lägesbild av informationssäkerhetshoten mot de finländska datanäten.

Vid användningen av de verksamhetsrättigheter som avses i 272 § i lagen om tjänster inom elektronisk kommunikation, vare sig det är ett företag, en sammanslutning eller en myndighet som sörjer för informationssäkerheten eller om det sker inom ramen för HARAVO-systemet, är det tekniskt sett i mångt och mycket fråga om en liknande filtrering av datatrafiken på basis av sökbegrepp och fortsatt behandling av meddelanden som kommit fram i filtreringen som när det gäller underrättelseinhämtning som avser datatrafik. I verksamhet enligt 272 § i lagen om tjänster inom elektronisk kommunikation används som sökbegrepp bland annat sådana identifieringsuppgifter som beskriver innehållet i skadeprogram, identifieringsuppgifter för teleadresser som använts för att sprida skadeprogram och sådana identifieringsuppgifter som beskriver trafikeringssätt som är typiska för skadeprogrammen. Frågan om huruvida man i verksamheten verkligen förmår upptäcka trafiken av skadeprogram som hotar den nationella sä-

kerheten beror på kvaliteten på de identifieringsuppgifter för skadeprogram som används som sökbegrepp vid filtreringen.

De identifieringsuppgifter för skadeprogram som används i företagens, sammanslutningarnas och myndigheternas verksamhet är i regel sådana som är kommersiellt eller i övrigt allmänt tillgängliga. De identifieringsuppgifter som matas in i HAVARO-systemet baserar sig i huvudsak på sådana uppgifter som Kommunikationsverkets Cybersäkerhetscenter har fått inom ramen för det samarbete som det bedriver både inom landet och internationellt. Bland Cybersäkerhetscentrets viktigaste internationella samarbetspartner finns de så kallade GovCERT-grupperna, som verkar inom de olika ländernas statsförvaltningar.

De skadeprogram som är svårast att upptäcka och som samtidigt orsakar störst skada för den nationella säkerheten är de statliga spionageprogrammen och andra skadeprogram. Möjligheterna är begränsade när det gäller att upptäcka sådana här skadeprogram, både inom ramen för de informationssäkerhetsåtgärder som företagen, sammanslutningarna och myndigheterna själva vidtar och med hjälp av HAVARO-systemet. Orsaken är framför allt att sådana identifieringsuppgifter som är nödvändiga för att upptäcka spionage och annan fientlig statlig verksamhet inte är tillgängliga för de verksamhetsberättigade aktörer som avses i 272 § i lagen om tjänster inom elektronisk kommunikation och de kan inte heller matas in i HAVARO-systemet. De identifieringsuppgifter som behövs för att upptäcka verksamheten är sådan information med hög skyddsnivå som man vanligen utbyter inom det internationella samarbetet mellan säkerhets- och underrättelsetjänster. Detta samarbete grundar sig på ömsesidigt förtroende mellan parterna. Villkoret för informationsutlämning inom ramen för samarbetet är nästan undantagslöst ett förbud mot att vidareöverlåta uppgifterna till utomstående. Eftersom Kommunikationsverkets Cybersäkerhetscenter, som driver HAVARO-systemet, inte är och inte kan vara part i samarbetet mellan säkerhets- och underrättelsetjänsterna, utan räknas som utomstående ur samarbetets perspektiv, kan inte de identifieringsuppgifter som skulle ha störst betydelse för skyddet av den nationella säkerheten lämnas ut till HAVARO-systemet.

Syftet med de informationssäkerhetsåtgärder som är möjliga med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation, HAVARO inbegripet, är att upprätthålla informationssäkerheten genom att skydda enskilda organisationer mot kränkningar. Syftet med åtgärderna är inte att tillgodose de informationsbehov som ansluter sig till bekämpningen av verksamhet som äventyrar den nationella säkerheten. För den som vidtar informationssäkerhetsåtgärder är inte sådan information som är väsentlig med tanke på upprätthållandet av den nationella säkerheten, såsom orsakerna till, omständigheterna kring, personerna bakom och bakgrundsmotiven till de allvarligaste informationssäkerhetskränkningarna, av någon central betydelse.

Ovan konstaterades det att den verksamhet som avses i 272 § i lagen om tjänster inom elektronisk kommunikation tekniskt sett nära påminner om verksamheten i jämförelsestaterna. Sådan verksamhet kan med en gemensam benämning kallas underrättelseinhämtning som avser datatrafik. Av den tekniska likheten i funktionerna följer att ett system med underrättelseinhämtning som avser datatrafik som grundar sig på filtrering av datatrafiken med hjälp av sökbegrepp även kan användas för identifiering av skadeprogram.

I jämförelsestaterna har underrättelseinhämtning som avser datatrafik en viktig ställning inte bara inom traditionell underrättelseinhämtning som gäller verksamhet som hotar den nationella säkerheten, utan också som metod för att upptäcka och skydda sig från cyberhot (t.ex. det svenska betänkandet ”En anpassad försvarsunderrättelseverksamhet”. Departementsserien 2005:30. Regeringskansliet/Försvarsdepartementet, s. 96–99). Underrättelseinhämtning som avser datatrafik möjliggör framför allt upptäckt av de cyberhot som på det allvarligaste sättet äventyrar samhällets viktigaste säkerhetsintressen.

Metoder av observationskaraktär

Bestämmelser om de metoder av observationskaraktär som polisen använder för att förhindra och avslöja brott och för att avvärja fara finns i polislagens 5 kap. Till de metoder som är av observationskaraktär hör observation, systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, teknisk spårning, teknisk observation av utrustning och inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, samt installation och avinstallation av anordningar, metoder eller programvara som stöder dessa metoder.

De metoder som är av observationskaraktär är med anledning av sin effektivitet och hur de fungerar samt att de bara innebär ett milt ingripande i de grundläggande rättigheterna viktiga metoder för underrättelseinhämtning inom civil underrättelseinhämtning. Syftet med befogenheterna för underrättelseinhämtning är att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten. Metoder av observationskaraktär spelar en viktig roll vid informationsinhämtning. Om de befogenheter som används inom civil underrättelseinhämtning riktas in på rätt sätt i ett så tidigt skede som möjligt, minskar antalet personer som kommer att beröras av underrättelseinhämtningen.

I synnerhet med sådan information i realtid som man får med hjälp av metoder av observationskaraktär kan man avsevärt förbättra lägesbilden av den nationella säkerheten och därigenom underlätta beslutsfattandet om hur den civila underrättelseinhämtningen ska riktas in och om dess prioriteringar. Med hjälp av information som inhämtats genom metoder av observationskaraktär kan man också öka effektiviteten i den civila underrättelseinhämtningen.

En egenskap hos de hemliga metoder för informationsinhämtning som är av observationskaraktär är att de ska fokuseras på en viss person. I ett beslut om teknisk avlyssning ska dessutom den lokal eller annan plats som avlyssningen gäller nämnas. I ett beslut om teknisk spårning ska det föremål, det ämne eller den egendom som spårningen riktas mot nämnas och vid teknisk observation av utrustning ska den tekniska anordning eller programvara som åtgärden riktas mot nämnas.

Vid användningen av sådana befogenheter som får användas i underrättelseinhämtningssyfte är det inte fråga om åtgärder för att förhindra, avslöja eller utreda brott, och även om det skulle vara fråga om verksamhet som allvarligt hotar den nationella säkerheten spelar preciseringen av en persons identitet inte en så betydande roll som då de befogenheter som grundar sig på ett brott används. Det är inte nödvändigt att en viss person identifieras i alla situationer, i synnerhet då man genom underrättelseinhämtning försöker hitta så att säga dolda hot som myndigheterna inte känner till förrän de framträder som fenomen eller planer. När det gäller befogenheterna för underrättelseinhämtning kommer det inte att finnas något grundat behov av att bedöma de särskilda förutsättningarna för att använda befogenheterna på ett sätt som motsvarar nuläget, såsom om det finns skäl att misstänka att personen i fråga har gjort sig skyldig till ett brott som överskrider ett visst sanktionshot eller om hen kan antas göra sig skyldig till ett sådant. Syftet med användningen av de befogenheter som får användas vid underrättelseinhämtning kan till exempel vara informationsinhämtning om hur en grupp är organiserad, vilka personer som hör till gruppen, hur aktiv gruppen är i ett visst område och vilka olika uttryck gruppens verksamhet tar sig. Informationen kan ha betydelse i såväl det operativa beslutsfattandet som i de beslut som fattas av statens högsta ledning. Av bland annat de orsaker som nämnts bör även befogenheter av observationskaraktär kunna riktas in på en begränsad grupp personer.

Bestämmelser om *förtäckt inhämtande av information* infördes första gången i den gällande polislagen och tvångsmedelslagen. Med förtäckt inhämtande av information avses inhämtande

av information genom kortvarig interaktion med en viss person där falska, vilseledande eller förtäckta uppgifter används för att hemlighålla polismannens uppdrag.

Eftersom befogenheterna används under så kort tid placerar sig förtäckt inhämtande av information någonstans mellan systematisk observation och täckoperationer. Metoden har klart gemensamma drag med täckoperationer, men verksamheten leder inte till samma sorts förtroende mellan aktören och objektet. Täckoperationer kan för närvarande på grundval av ett brott riktas in på en viss person, som inte behöver vara den person som man kan anta kommer att göra sig skyldig till ett brott. Föremålet för förtäckt inhämtande av information bör vid underrättelseverksamhet även kunna vara en grupp personer, även om den egentliga interaktionen och mötet med personer funktionsmässigt måste riktas in på enskilda personer i gruppen.

Det primära målet med *optisk observation* är att producera sådana bilder som vid behov kan användas till exempel vid analys av information, eller så kan bildmaterialet ha egen betydelse. I vissa situationer kan man pruta på bildkvaliteten, såsom då man behöver få information enbart om hur vissa personer eller grupper rör sig i ett visst område. Genom optisk observation kan man ersätta en betydande del av den arbetsinsats som annars skulle behövas. Ett exempel på detta är då en eller flera byggnader eller objekt i terrängen behöver bevakas dygnet runt och poliserna vid skyddspolisen inte kan sköta bevakningen på grund av objektets särdrag.

När det gäller civil underrättelseinhämtning är det väsentligt att man får in så aktuell och specifik information som möjligt om innehållet i kommunikation. *Teknisk avlyssning* möjliggör omfattande och detaljerad informationsinhämtning om verksamhet som allvarligt hotar den nationella säkerheten samt om personer och grupper som är kopplade till sådan verksamhet. Vid teknisk avlyssning är syftet också att identifiera en viss person eller grupp eller att inhämta information om deras verksamhet.

Övervakning av personers, gruppers och transporters (föremål, ämnen eller egendom) rörelser med hjälp av teknisk spårning ger skyddspolisen möjligheter att planera och rikta in sina åtgärder. *Teknisk spårning av något annat än en person* skiljer sig från optisk observation och teknisk avlyssning i synnerhet på så sätt att det inte lika kraftigt ingriper i de grundläggande rättigheterna och mänskliga rättigheterna. Genom ändamålsenlig teknisk spårning kan man komplettera den normala observation som skyddspolisen utför vid civil underrättelseinhämtning. Det är emellertid skäl att nämna att teknisk spårning, på samma sätt som optisk observation och teknisk avlyssning, inte i alla situationer helt kan ersätta de iakttagelser som görs av en polis. Teknisk spårning av en person ingriper däremot i de grundläggande rättigheterna och mänskliga rättigheterna, såsom rörelsefriheten och skyddet för privatlivet.

Med *teknisk observation av utrustning* avses att en funktion, informationsinnehållet eller identifieringsuppgifterna i en dator eller i en liknande teknisk anordning eller i dess programvara på något annat sätt än enbart genom sinnesförnimmelser observeras, upptas eller behandlas på något annat sätt för att utreda omständigheter som är av betydelse för förebyggande av ett brott.

Arbetsgruppen för en informationsanskaffningslag har föreslagit att det ska införas bestämmelser om underrättelseinhämtning som avser utländska datasystem, med vilket man avser sådan underrättelseinhämtning som sker med datatekniska metoder och som gäller uppgifter som behandlas i datasystem i utlandet. I praktiken omfattar underrättelseinhämtning som avser datasystem befogenheter som gäller teknisk avlyssning och teknisk observation av utrustning.

Enligt 5 kap. 23 § 2 mom. i polislagen får information om innehållet i ett meddelande eller om sådana identifieringsuppgifter som avses i 8 § inte inhämtas genom teknisk observation av utrustning. En motsvarande bestämmelse finns i 10 kap. 23 § 2 mom. i tvångsmedelslagen. Av

polislagen och tvångsmedelslagen och förarbetena till dem framgår det indirekt att man i dessa bestämmelser med innehållet i ett meddelande uttryckligen avser sådant innehåll i ett meddelande som framkommer i samband med teleavlyssning och teknisk avlyssning. Det är med andra ord fråga om kommunikation i realtid mellan två personer, till exempel via dator eller smarttelefon. Följaktligen omfattas sådana dokument som redan har upptagits eller sparats på den enhet som använts vid kommunikationen och som inte är i kontakt i realtid med teknisk avlyssning eller teleavlyssning av teknisk observation av utrustning.

Teknisk observation av utrustning gör det möjligt att rikta in underrättelseinhämtningen till exempel på att utreda sådana dokument som finns på en dator. Teknisk observation av utrustning skulle vara en nödvändig befogenhet till exempel i samband med platsspecifik underrättelseinhämtning, om man skulle behöva inhämta uppgifter i digital form ur dokument som finns på en teknisk enhet.

De befogenhetsbestämmelser som ska gälla vid civil underrättelseinhämtning måste kunna möta de utmaningar som den tekniska utvecklingen i verksamhetsmiljön medför, och detta måste beaktas vid bedömningen av den gällande lagstiftningen. Detta gäller såväl de metoder som används som den verksamhet som är objektet för metoderna.

Även när det gäller civil underrättelseinhämtning behövs det bestämmelser som gäller befogenheterna i fråga om *inhämtning av identifieringsuppgifter för teleadresser och teleterminalutrustning*. Genom denna metod kan man inhämta information som gör att användningen av sådana befogenheter som ingriper i skyddet för förtroliga meddelanden (teleavlyssning och teleövervakning) är möjlig att rikta in på ett föremål för civil underrättelseinhämtning, en teleadress eller teleterminalutrustning som innehas av en viss person, vilket skulle bidra till att förbättra skyddet av de grundläggande rättigheterna för utomstående.

Bestämmelsen om *installation och avinstallation av anordningar, metoder eller programvara* är framför allt en bestämmelse som möjliggör teknisk observation. Teknisk observation skulle i praktiken ofta vara omöjlig eller åtminstone mycket svår att genomföra utan denna befogenhet. I synnerhet när det gäller underrättelseinhämtning som avser utländska förhållanden är det nödvändigt att installation och avinstallation av anordningar, metoder eller programvara är möjlig även i samband med teleavlyssning och teleövervakning, eftersom användningen av dessa metoder i princip förutsätter en begäran om att en teleoperatör ska göra de kopplingar som behövs eller lämna ut uppgifter. När det gäller underrättelseinhämtning som avser utländska förhållanden är det ändamålsenligt att de aktuella befogenheterna tillämpas med myndighetens egen utrustning.

Täckoperation och bevisprovokation genom köp

Enligt 5 kap. 28 § 1 mom. i polislagen avses med täckoperation planmässigt inhämtande av information om en viss person eller dennes verksamhet genom infiltration, där falska, vilseledande eller förtäckta uppgifter eller registeranteckningar används eller falska handlingar framställs eller används för att förvärva förtroende som behövs för inhämtandet av information eller för att förhindra att inhämtandet av information avslöjas. I definitionen nämns inte särskilt en grupp av personer. De personer som propositionen och ett beslut om täckoperation förutsätter att ska specificeras kan naturligtvis utgöra en grupp. Tidigare var det möjligt att rikta en täckoperation mot en grupp personer.

Nu för tiden måste de personer som är föremål för en täckoperation kunna specificeras åtminstone med hjälp av uppgifter om dem i anslutning till den brottsliga verksamheten. Detta förutsätter för sin del inte att de enskilda personerna namnges. I civil underrättelseverksamhet bör täckoperationer kunna riktas även mot en viss grupp personer, där täckoperationen inte

riktas mot varje enskild person som bildar gruppen. I vissa fall behöver man inte inhämta information om en enskild persons aktivitet. Det kan vara nödvändigt att infiltrera till exempel en bestämd avgränsad grupp människor och på så sätt inhämta information om en bakgrundsorganisation som styr deras verksamhet och personer i den organisationen. Det kan till exempel gälla en statlig grupp av personer som utövar hybridpåverkan på förhållanden i Finland.

För täckoperationer och bevisprovokation genom köp förutsätts att metoden är nödvändig för att ett brott ska kunna förhindras eller avslöjas. En förutsättning för bruk av täckoperation är dessutom att inhämtandet av information måste anses nödvändigt på grund av att den brottsliga verksamheten är planmässig, organiserad eller yrkesmässig eller kan väntas fortsätta eller upprepas. Det är motiverat att ange lika strama villkor för bruket av täckoperation och bevisprovokation genom köp som underrättelsemetoder även i samband med civil underrättelseverksamhet trots att syftet med dem inte är att inhämta information för att förhindra, avslöja och utreda brott.

I 5 kap. 29 § i polislagen föreskrivs det om brottsförbud som i strid med paragrafens rubrik innehåller rätten för en polisman som utför en täckoperation att begå mindre förseelser. I 5 kap. 30 § i lagen finns bestämmelser om deltagande i en organiserad kriminell sammanslutnings verksamhet och i kontrollerade leveranser. Enligt bestämmelsen kan en polisman som företar en täckoperation under sitt deltagande i en organiserad kriminell sammanslutnings verksamhet skaffa lokaler, fordon eller andra sådana hjälpmedel, transportera personer, föremål eller ämnen, sköta ekonomiska angelägenheter eller bistå den kriminella sammanslutningen på andra jämförbara sätt. Polismannen går fri från straffansvar, om det på synnerligen giltiga skäl har kunnat antas att: 1) åtgärden genomförs också utan polismannens medverkan, 2) polismannens verksamhet inte äventyrar eller skadar någons liv, hälsa eller frihet eller orsakar betydande fara för eller skada på egendom, och 3) biståndet avsevärt främjar möjligheterna att uppnå syftet med täckoperationen.

Enligt den senare bestämmelsen kan med andra ord en polisman som utför en täckoperation genom att delta i en organiserad kriminell sammanslutnings verksamhet delvis begå straffbara handlingar som räknas upp i 17 kap. 1 a § i strafflagen. Straffbestämmelsen nämns inte i paragrafen om befogenhet, men det kan även bli fråga om befrielse från ansvar för medhjälp till brott.

Täckoperationer och bevisprovokation genom köp är metoder som redan i nuläget i första hand anses som typer av underrättelseinhämtning och inte nödvändigtvis som en del av en förundersökning. Också Europadomstolen har tolkat okonventionella metoder som polisen använder för inhämtande av information uttryckligen som underrättelseinhämtning som delvis bedöms enligt annorlunda kriterier än förfarandet vid rättegångar i brottmål eller vid förundersökningar som en del av det. När metoderna bedöms ur perspektivet civil underrättelseverksamhet ligger ståndpunkten ännu längre från brott, och användning av befogenheter som grundar sig på brott ska inte alls komma på fråga. Bland annat av dessa skäl är det inom civil underrättelseverksamhet inte heller på samma sätt nödvändigt att delta i en organiserad kriminell sammanslutnings verksamhet eller utföra brott av förseelsetyp. Om ett sådant behov uppstår bör befogenheterna i polislagens 5 kap. (eller tvångsmedelslagens 10 kap.) tillämpas.

Den ståndpunkt som förvaltningsutskottet en gång i tiden framförde (FvUB 17/2000) om utgångspunkterna för bevisprovokation genom köp och om stark sekretess motsvarar den ståndpunkt som förundersökningsmyndigheterna numera företräder. Utskottets ställningstagande har sedermera åtminstone inom polisväsendet omfattats i princip vad gäller hur man förhåller sig till bevisprovokation genom köp. Förvaltningsutskottet har ansett att redan blotta vetskapen om att täckoperation eller bevisprovokation genom köp har använts kan leda till att detaljer i verksamheten avslöjas. Enligt förvaltningsutskottets åsikt sätts den åtalades rätt att få en

rättvis rättegång inte på spel när uppgifter om täckoperation eller bevisprovokation genom köp inte används för att motivera åtalsprövning eller vid rättegången, utan bara hjälper polisen att orientera sig rätt i utredningen.

Den nämnda utgångspunkten visar att det finns en märkbar principiell skillnad mellan bevisprovokationer genom köp och täckoperationer i förhållande till vårt straffprocessrättsliga system som bygger på legalitetsprincipen. Motsvarande spänning kan inte anses ingå i täckoperation och bevisprovokation genom köp som används för underrättelseinhämtning och vilkas egentliga syfte inte är att inhämta information för en straffprocess eller för annat syfte än att rikta verksamheten hos myndigheten för underrättelseinhämtning. Trots denna grund för förutsättningen att utgångspunkten för att använda bevisprovokation genom köp och täckoperation är stark sekretess nödvändig av säkerhetsskäl och med tanke på att underrättelseinhämtningsoperationer ska ge resultat. Om bevisprovokation genom köp avslöjas kan det medföra hot mot infiltratörens liv eller hälsa i form av hämndaktioner. Hämndaktionerna kan även riktas mot polismannens närstående samt mot utomstående personer som eventuellt har varit informationskällor för skyddspolisen eller på annat sätt främjat underrättelseinhämtningen. Att bevisprovokation genom köp och täckoperationer hemlighålls är också förståeligt, för om föremålen för sådana åtgärder alltid informeras om dem skulle det bli omöjligt att utreda till exempel en terroristorganisation och cellerna som hör till den. Heltäckande sekretess i fråga om bevisprovokation genom köp och täckoperationer kan visa sig vara problematisk i fall där information som inhämtats genom metoderna framskrider till att användas som bevis. Detta beaktas i 5 a kap. 44 § som föreslås i polislagen.

När man beaktar att en täckoperation utförs genom infiltration och särdragen i underrättelseinhämtningen kan en hänvisning till 5 kap. 29 § i polislagen dock inte anses tillräcklig. Enligt 12 kap. i strafflagen som gäller landsförräderibrott är sådana brott straffbara vilkas rekvisit kan uppfyllas genom kontakten i en täckoperation. I många fall är det inte så, eftersom tjänstemannen som utför täckoperationen inte har den avsikt som förutsätts i straffbestämmelsen i kapitlet eller eftersom gärningen inte leder till följder som avses i straffbestämmelsen. Å andra sidan tillämpas till exempel 12 kap. 3 § i strafflagen bland annat i fall där en finsk medborgare i vissa hotfulla situationer, det vill säga under en militär eller internationell politisk kris som berör Finland eller när ett överhängande hot om en sådan kris föreligger, inleder samarbete med fienden. Det är å sin sida som olovlig underrättelseverksamhet (strafflagen 12 kap. 9 §) straffbart till exempel att en gärningsman i avsikt att skada en främmande stat skaffar upplysningar om en främmande stats försvar eller säkerhet eller om omständigheter med omedelbar inverkan på dem och därigenom skadar eller äventyrar Finlands utrikesrelationer. I 12 kap. 11 § i strafflagen finns dessutom en straffbestämmelse om upprätthållande av landsförrädisk förbindelse som täcker förbindelse med en främmande stat eller dess agent för att begå ett brott som avses i kapitlet.

Hur täckoperationer som används i underrättelseinhämtning förhåller sig till bestämmelserna i 12 kap. i strafflagen kan inte baseras på rättspraxis. Å andra sidan ska det beaktas att alla sätt att begå landsförräderibrott enligt 12 kap. i strafflagen inte är bundna enbart till umgänge med en annan person eller en grupp av personer vilket är utmärkande för täckoperationer. Spioneri enligt 12 kap. 5 § i strafflagen kan genomföras även med tekniska metoder för inhämtande av information. Också aktivitet enligt lagen om underrättelseinhämtning avseende datatrafik kan riktas mot en främmande stats datatrafik. Därför bör gränsen inte dras enbart vid täckoperationer utan mer allmänt vid underrättelseinhämtning, det vill säga vid användning av metoder för underrättelseinhämtning enligt 5 a kap. som föreslås i polislagen och i lagen om civil underrättelseinhämtning som föreslås. Eftersom motsvarande metoder för inhämtande av information tas i bruk även inom militär underrättelseinhämtning (lag om militär underrättelseverksamhet som föreslås) gäller samma aspekter även metoder som används inom militär underrättelseverksamhet. För tydlighetens skull är det motiverat att dra en gräns mellan gär-

ningar som är straffbara enligt 12 kap. i strafflagen och bruk av metoder för underrättelseinhämtning genom att lägga till en bestämmelse om gränsdragningen i slutet av kapitlet.

Kontrollen av hur kraven på förfaringssätten vid täckoperationer och bevisprovokation genom köp följs blir i praktiken ofta en intern uppgift. Även när täckoperationer och bevisprovokation genom köp används för underrättelseinhämtning är det viktigt att i verkligheten och på ett effektivt sätt kontrollera verksamheten. Att pröva gränserna för verksamhetens laglighet får inte lämnas till den verkställande nivån. De måste godkännas av dem som ansvarar för den operativa verksamheten.

Strukturerna för kontrollen av täckoperationer och bevisprovokation genom köp ska vara klara innan verksamheten inleds. Utöver den interna kontrollen och den som inrikesministeriet utför kommer en oberoende rättslig övervakare, underrättelseombudsmannen, att ha en viktig roll i tillsynen över täckoperationer och bevisprovokation genom köp, liksom i övervakningen av andra metoder för underrättelseinhämtning.

Styrd användning av informationskällor och deras säkerhet

Användning av styrda informationskällor regleras i 5 kap. 40 § i polislagen. I paragrafens 1 mom. finns en definition av informationskällor. Enligt den avses med användning av informationskällor annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötsel av i 1 kap. 1 § i polislagen avsedda uppgifter av personer som inte hör till polisen eller till någon annan förundersökningsmyndighet.

Den nuvarande lagstiftningen gör det möjligt att hemlighålla kontakten mellan en informationskälla och en polisman som inhämtar information enligt 5 kap. 46 § i polislagen (skyddande av inhämtande av information) under vissa villkor. Informationskällan kan dock inte med stöd av bestämmelsen till exempel ges en ny identitet. Syftet är att skydda verksamheten och även informationskällan genom tjänstemännen som utför arbetet. Sålunda kan endast tjänstemän ges sådant skydd som avses i denna paragraf och endast tjänstemän kan använda sig av det för att skydda informationsinhämtningen.

Skyddspolisen är i princip skyldig att enligt behov sörja för sina informationskällors säkerhet under och efter informationsinhämtningen. Det finns dock ingen lagstiftning om föregripande skydd av informationskällan. Informationskällorna för underrättelseinhämtningen kan i vissa fall sätta sitt eget liv och sin hälsa på spel. Man måste förhålla sig särskilt allvarlig när källan till hot mot informationskällans liv och hälsa är en statlig aktör. Det kan till exempel gälla att en person söker politisk asyl, varvid staten i ursprungslandet kan ha stort intresse av att påverka aktiviteten hos personen som är informationskälla. Då kräver skyddet av informationskällan ett annat slag av intensitet än vid verksamhet med informationskällor enligt 5 kap. Skyddspolisen bör kunna skydda en eventuell informationskälla redan i preventivt syfte för att källan ska kunna lita på att den får det skydd som behövs. Vid behov av långvarigt skydd och som sista utväg bör man överväga användning av vittnesskyddsprogram som regleras i lagen om vittnesskyddsprogram (65/2014). På grund av vad som nämns ovan behöver det regleras om skyddet av informationskällan vilket kan inledas i preventivt syfte.

Vid kontrollerad leverans är det nästan utan undantag fråga om att transporten av föremål, ämnen eller egendom som innehas olagligt övervakas och syftet är att genom att ingripa senare utreda allvarlig och ofta även organiserad brottslighet som ligger bakom. Vid kontrollerad leverans kan syftet vara att utreda hela distributionskedjan och var transporten slutligen hamnar. Fördröjt ingripande har nästan uteslutande att göra med att en transport som kontrolleras innehåller last som det är straffbart att inneha, eller det uppfyller rekvisitet för brott av förberedande natur till exempel i fråga om tillverkning av produkter med dubbel användning.

Vid underrättelseinhämtningen är syftet i princip inte att inhämta information om brott utan befogenheterna på grund av ett brott regleras separat. Kontrollerad leverans behöver därför inte regleras som en metod för underrättelseinhämtning.

Beslutsfattande

Beslutanderätten om användning av vissa hemliga metoder för inhämtande av information är på det sätt som beskrivits i föregående avsnitt i delarna om lagstiftning och praxis fördelat på domstol eller på en anhållningsberättigad polisman. Till domstolens beslutanderätt hör följande hemliga metoder för inhämtande av information som avses i 5 kap. i polislagen: teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, teknisk avlyssning till vissa delar, optisk observation till vissa delar, teknisk spårning till vissa delar och teknisk observation av utrustning. I brådskande situationer där polisen tillfälligt själv kan besluta om användning av befogenheter som hör till domstolens beslutanderätt ska ärendet föras till domstol så snart som möjligt, dock senast 24 timmar efter det att användningen av metoden har inletts. Polisen kan dock besluta om vissa hemliga metoder för inhämtande av information för att avvärja hot mot liv eller hälsa samt med en persons samtycke teleövervakning vid misstanke om brott som direkt har samband med en teleadress eller teleterminalutrustning.

Polisen beslutar självständigt om systematisk observation, förtäckt inhämtande av information, anskaffning av identifieringsuppgifter för en teleadress eller en teleterminalutrustning, täckoperationer och bevisprovokation genom köp, styrd användning av informationskällor samt användning av kontrollerade leveranser.

Ett yrkande om tillstånd som hör till domstolens beslutanderätt och som gäller hemligt inhämtande av information ska enligt 5 kap. 45 § i polislagen utan dröjsmål tas upp till behandling i domstol i närvaro av den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman som är insatt i ärendet. Ärendet ska avgöras skyndsamt. Ärendet får avgöras utan att den person hörs som med fog kan antas begå eller har begått brottet, och i regel utan att innehavaren av teleadressen eller teleterminalutrustningen hörs.

Ett beslut i ett tillståndsärende som gäller hemliga metoder för inhämtande av information får inte överklagas genom besvär. Klagan mot beslutet får anföras utan tidsbegränsning.

Den som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning och teleövervakning ska enligt 5 kap. 58 § i polislagen utan dröjsmål underrättas om detta efter det att syftet med inhämtandet av information har nåtts. Personen i fråga ska dock underrättas om det hemliga inhämtandet av information senast ett år efter att det har upphört. Domstolen kan dock på yrkande av en anhållningsberättigad polisman besluta att underrättelsen till den som varit föremål för åtgärden får skjutas upp högst två år åt gången. Villkoret för att underrättelsen ska skjutas upp är att det är motiverat för att trygga pågående inhämtning av information, trygga statens säkerhet eller skydda liv eller hälsa. Domstolen får besluta att underrättelsen ska utebli, om det är nödvändigt för att trygga statens säkerhet eller skydda liv eller hälsa.

I praktiken beviljar domstolen tillstånd för användning av teleavlyssning och teleövervakning i merparten av fallen. Det uppskattas att några negativa beslut fattas årligen. År 2015 förkastade domstolarna 11 yrkanden från polisen om teletvångsmedel som alla gällde ansökningar enligt tvångsmedelslagen.

När regleringen av beslutsfattandet om metoder för underrättelseinhämtning övervägs är det inte motiverat att avvika från valen för användning av hemliga metoder för inhämtande av in-

formation enligt polislagens 5 kap. Det är även motiverat att till den delen bygga upp 5 a kap. i polislagen så att den till de väsentliga delarna baseras på bestämmelserna i 5 kap. En synpunkt som betonar påtagliga ingrepp i grundläggande och mänskliga rättigheter talar för att domstolens nuvarande tillgängliga befogenhet att fatta beslut om hemliga metoder för inhämtande av information till stor del ska förbli den samma som i nuläget. Ingripanden i grundläggande och mänskliga rättigheter vad gäller befogenheter att fatta beslut har bedömts för varje metod i samband med reformen av lagstiftningen om förundersökning och tvångsmedel (Justitieministeriets kommittébetänkande 2009:2) inklusive grundlagsutskottets ställningstaganden. Därför är det också motiverat att i fråga om beslutsfattandet om metoderna för underrättelseinhämtning i 5 a kap. så långt som möjligt följa den lagstiftning som tillämpats i 5 kap.

Utöver metoderna för underrättelseinhämtning ska det regleras om beslutandet om underrättelseinhämtning utomlands. Utgångspunkten är att domstolen inte har behörighet att besluta om användning av befogenheter på annat håll än i Finland. Det är inte heller ändamålsenligt att föra över operativt beslutsfattande i det juridiska systemet till nya aktörer på grund av de utrikespolitiskt sett sensitiva element som hänför sig till underrättelseinhämtning utomlands. I en del länder som ingår i den internationella jämförelsen beslutar chefen för underrättelseverket om underrättelseinhämtning utomlands. Det är motiverat att reglera på samma sätt om beslutsfattande om underrättelseinhämtning utomlands inom civil underrättelseverksamhet. Chefen för skyddspolisen beslutar också i nuläget om användningen av de kraftigaste metoderna, täckoperation och bevisprovokation genom köp. I bedömningen för beslut om dem ingår i fråga om allvar motsvarande typer av omständigheter som i underrättelseinhämtning utomlands.

Det är också motiverat att av de nämnda orsakerna reglera bestämmelserna om underrättelse om användning av metoder för inhämtning på motsvarande sätt som i polislagens 5 kap. med beaktande av särdragen i civil underrättelseverksamhet.

Gemensamma bestämmelser för alla hemliga metoder för inhämtande av information

Skyddande av hemligt inhämtande av information

Bestämmelser om skyddande av hemligt inhämtande av information finns i 5 kap. 46 § i polislagen. Paragrafens 1 mom. gäller polisens möjlighet att dröja med att ingripa i ett brott när den använder hemliga metoder för att inhämta information. Villkoret är att fördröjningen inte orsakar betydande fara för någons liv, hälsa eller frihet eller avsevärd risk för betydande miljö-, egendoms- eller förmögenhetsskada. Det förutsätts dessutom att fördröjningen med att ingripa är nödvändig för att dölja att information inhämtas eller för att trygga verksamhetens syfte.

Enligt paragrafens 2 mom. får polisen använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt upprätta och använda falska handlingar, när det är nödvändigt för att skydda sådant hemligt inhämtande av information som redan genomförts, pågår eller kommer att genomföras.

Enligt nuvarande lagstiftning får skydd användas i alla hemliga metoder för inhämtande av information (även vid förtäckt inhämtande av information). Behovet av skydd kan uppstå till exempel vid teleövervakning som polisen utför med egna anordningar. Med stöd av momentet får dock inte täckmantel ges till en informationskälla eller till någon utomstående, utan syftet är att skydda verksamheten.

Oriktiga noteringar och anteckningar behandlas i riksdagens biträdande justitieombudsmans avgörande 571/2/08. Frågan har samband med att polisen är tvungen att utreda och att kravet

på lagenliga noteringar och intresset att hålla bevisprovokation genom köp och täckoperationer hemliga är sinsemellan motstridiga. Lagen ger inget klart svar till exempel på om man får och i vilken utsträckning man för att förhindra att en hemlig metod för informationsinhämtning avslöjas får upprätta oriktiga förundersökningsprotokoll eller underrättelser om utredningar.

Det är i många fall fråga om intresseavvägning och helhetsbedömning. Utgångspunkten är att starka skyddsmetoder inte bör användas på mycket lätta grunder på grund av de problem de medför och av rättssäkerhetsskäl. I princip medför ett oriktigt dokument från en myndighet även en oriktig registeranteckning i myndigheters register som åtnjuter allmänt förtroende. Därför ska det skydd som utförs vara nödvändigt.

Oriktiga anteckningar får dock inte lämnas i registren. Enligt 3 mom. anges skyldigheten att rätta registeranteckningarna.

Det finns ett utpräglat behov av motsvarande skydd för inhämtande av information som anges i de ovan nämnda 2 och 3 mom. även för att skydda civil underrättelseverksamhet. Utgångspunkten är att hela den civila underrättelseverksamheten ska kunna skyddas. Känsligheter av många slag hör till underrättelseverksamhet, och föremålet för verksamheten kan vara en annan stats förvaltning, en enskild person eller en grupp av personer av högt intresse, en industrigren eller ett enskilt företag. I praktiken försöker man genom underrättelseinhämtning inhämta information utan att föremålet vet om det och mot föremålets vilja. För att minimera risken att avslöjas bör det vara möjligt att använda skydd redan i ett tidigt skede. Till exempel skyddet av en tjänsteman som utför en uppgift inom underrättelseinhämtning genom infiltration i en viss organisation kräver mycket intensiva skyddsåtgärder och att de inleds i ett mycket tidigt skede. Vid användning av skydd i civil underrättelseverksamhet finns det inte heller motsvarande problem med rättssäkerheten som när befogenheter används på grund av brott, för i civil underrättelseverksamhet är det principiella syftet att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten.

Yppandeförbud

I polislagens 5 kap 48 § föreskrivs det om yppandeförbud som gäller hemliga tvångsmedel. Av 1 mom. i paragrafen framgår det att yppandeförbud inte får meddelas vem som helst, till exempel en invånare i ett bostadsaktiebolag eller någon annan utomstående som råkar upptäcka installation av utrustning för teknisk observation. Det förutsätts dessutom att den utomstående med anledning av sitt uppdrag eller sin ställning har bistått eller blivit ombedd att bistå vid användningen av en metod för underrättelseinhämtning. Yppandeförbud kan enligt 2 mom. i paragrafen meddelas för högst ett år åt gången. Förbudet ska meddelas mottagaren skriftligen och bevisligen för kännedom och i det ska specificeras de omständigheter som förbudet omfattar, nämnas förbudets giltighetstid och anges hotet om straff för överträdelse av förbudet.

Vid användning av metoder för underrättelseinhämtning kan man råka ut för situationer där det är nödvändigt att anlita utomstående hjälp. Till exempel för installation av utrustning för teknisk observation kan det behövas utomstående sakkunskap eller tjänster av servicebolaget för en byggnad. På så sätt kan utomstående få information som om den röjs kan äventyra användningen av metoden för underrättelseinhämtning och hela underrättelseverksamheten. Avsikten med yppandeförbudet är att skydda användningen av metoden för underrättelseinhämtning och att underrättelseverksamheten avslöjas, men även sekretessbelagda taktiska och tekniska metoder. Det behöver regleras om yppandeförbud även i samband med metoder för underrättelseinhämtning.

Förbud mot avlyssning och observation

Förbud mot avlyssning och observation regleras i 5 kap. 50 § i polislagen. Enligt paragrafen gäller i fråga om förbud som avser teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation i tillämpliga delar 10 kap. 52 § i tvångsmedelslagen.

Enligt 10 kap. 52 § 1 mom. i tvångsmedelslagen får teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation inte riktas mot meddelanden mellan 1) en misstänkt och hans eller hennes rättsliga biträde som avses i 17 kap. 13 § 1 eller 3 mom. i rättegångsbalken eller tolk som avses i 1 mom. i den paragrafen, eller den som till det rättsliga biträdet står i sådant förhållande som avses i 22 § 2 mom. i det kapitlet, 2) en misstänkt och en i 17 kap. 16 i rättegångsbalken avsedd präst eller någon annan person i motsvarande ställning, eller 3) en misstänkt som berövats sin frihet på grund av brott och en läkare, en sjukskötare, en psykolog eller en socialarbetare. Om det enligt 3 mom. under tiden för teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation eller vid något annat tillfälle framkommer att det är fråga om ett meddelande som inte får avlyssnas eller observeras, ska åtgärden avbrytas och de upptagningar som fåtts genom åtgärden och anteckningarna om de uppgifter som fåtts genom den genast utplånas. Enligt 4 mom. gäller de förbud mot avlyssning och observation som avses i denna paragraf dock inte sådana fall där en person som avses i 1 eller 2 mom. är misstänkt för samma brott som den misstänkte eller ett brott som direkt anknyter till det brottet och det också i fråga om denne har fattats beslut om teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation.

De ovan relaterade förbuden mot avlyssning och observation har angetts med tanke på straffprocess och straffprocessuella tvångsmedel. Trots att förbud mot avlyssning och observation har en betydelsefull ställning också inom civil underrättelseverksamhet visar sig deras status på annat sätt än i en straffprocess. Inom den civila underrättelseverksamheten ska förbuden bedömas nästan uteslutande som förbud som står utanför straffprocessen, och som inte har någon omedelbar koppling till rättssäkerheten för den brottsmisstänkte. Genom metoderna för underrättelseinhämtning ingriper man emellertid på samma sätt i de grundläggande och mänskliga rättigheterna som genom hemliga metoder för inhämtande av information, trots att det egentliga syftet för metoderna för underrättelseinhämtning inte är straffprocessuell. För användningen av metoder för civil underrättelseverksamhet ska det regleras om förbud mot avlyssning och observation på samma sätt som vid användningen av övriga hemliga metoder för inhämtande av information.

Till åtskillnad från polis- och tvångsmedelslagen riktas metoden för underrättelseinhämtning inte mot en brottsmisstänkt eller mot en person som antas bli gärningsman för att förhindra, avslöja eller utreda brott. I civil underrättelseverksamhet är det fråga om att inhämta information om verksamhet som utgör ett allvarligt hot mot den nationella säkerheten. Det kan också vara svårt att identifiera ställningen och personrelationerna hos föremålen för civil underrättelseverksamhet i inledningsfasen och de nära relationer som avses i 17 kap. 17 § i rättegångsbalken har inte en lika betydelsefull ställning som i en straffprocess.

På grund av vad som är utmärkande för den civila underrättelseverksamheten bör det regleras att teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation inte får riktas mot sådan kommunikation, som parterna i kommunikationen inte får vittna om med stöd av 17 kap. 13, 14, 16, 20 § eller 22 § 2 mom. i rättegångsbalken. I 17 kap. 13 § i rättegångsbalken regleras ett rättegångsombud, ett rättegångsbiträde och en tolks plikt att inte utan lov vittna om vad han eller hon har fått veta vid skötseln av ett uppdrag i anslutning till en rättegång, vid lämnande av juridisk rådgivning som gäller huvud-

mannens rättsliga ställning vid förundersökning eller i någon annan handläggningsfas inför en rättegång, vid lämnande av juridisk rådgivning som gäller inledande eller undvikande av rättegång. Dessutom anges i paragrafen plikten för en advokat, ett rättegångsbiträde som avses i lagen om rättegångsbiträden med tillstånd eller ett offentligt rättsbiträde att olovligen vittna om en enskild persons eller en familjs hemlighet eller affärs- eller yrkeshemligheter som han eller hon har fått kännedom om i något annat uppdrag än ett sådant som avses ovan. I 17 kap. 14 § i rättegångsbalken anges att en läkare eller någon annan yrkesutbildad person inom hälso- och sjukvården inte får vittna om känsliga uppgifter om en enskild persons eller familjs hälsotillstånd eller någon annan hemlighet som gäller en enskild person eller familj och som han eller hon har fått kännedom om på grund av sin ställning eller uppgift, om inte den till vars förmån tystnadsplikten har föreskrivits ger sitt samtycke till det. I 17 kap. 16 § i rättegångsbalken anges skyldigheten för en präst eller någon annan person i motsvarande ställning att inte vittna om vad han eller hon har fått veta under bikt eller enskild själavård, om inte den till vars förmån tystnadsplikten har föreskrivits ger sitt samtycke till det. I 17 kap. 20 § i rättegångsbalken regleras rätten för upphovsmannen, utgivaren och utövaren av programverksamheten till ett meddelande som enligt lagen om yttrandefrihet i masskommunikation har gjorts tillgängligt för allmänheten att vägra vittna om vem som har lämnat de upplysningar som meddelandet grundar sig på samt om upphovsmannens identitet. I 17 kap. 22 § 2 mom. i rättegångsbalken utvidgas det personliga tillämpningsområdet av vissa av förbuden och rättigheterna att vittna som nämns ovan. Enligt bestämmelsen har den som har fått information som avses i 11 § 2 eller 3 mom., 13 § 1 eller 3 mom., 14 § 1 mom. eller 20 § 1 mom. när han eller hon var anställd hos eller annars biträdde den som avses i bestämmelsen i fråga motsvarande skyldighet eller rätt att vägra vittna som den som avses i bestämmelsen i fråga. Det är dock inte nödvändigt att utsträcka hänvisningen till att gälla 11 § 2 eller 3 mom. eftersom ett förbud enligt dem inte heller föreslås.

Dessutom behöver det regleras om åtgärder ifall det under avlyssning eller observation eller vid andra tidpunkter framgår att det är förbjudet att avlyssna eller observera meddelandet. Då ska åtgärden avbrytas och de upptagningar och anteckningar som gäller informationen som erhållits ska genast utplånas. För tydlighetens skull bör det även regleras separat om att förbudet återtas när det är källan till ett hot som är föremål för förbudet mot avlyssning eller observation.

Utlämnande av uppgifter till andra förundersökningsmyndigheter

Polislagen innehåller inga bestämmelser om överlåtelse av uppgifter till andra förundersökningsmyndigheter. Den närmaste förebilden är 5 kap. 54 § i polislagen där det föreskrivs om användning av överskottsinformation. Enligt 5 kap. 53 § i polislagen avses med överskottsinformation sådan information som fåtts genom teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter och teknisk observation, när informationen inte har samband med ett brott eller avvärjande av fara eller när den gäller något annat brott än det för vars förhindrande eller avslöjande tillståndet har getts eller beslutet fattats. Överskottsinformation kan med andra ord definieras som information som har erhållits som biprodukt vid användningen av laglig informationsinhämtning på så sätt att den inte varit det egentliga eller planerade syftet med åtgärden. Bestämmelserna om överskottsinformation utgör ett slags mellanläge mellan fri bevisföring enligt vilken bevis fritt får utnyttjas och begränsningarna som gäller förbud mot att vittna. Informationen kan gälla något brott eller något som inte alls har samband med brott, men som är betydelsefullt för myndighetens verksamhet.

Enligt 5 kap. 54 § 1 mom. i polislagen får överskottsinformation användas i samband med utredning av brott, när informationen gäller ett brott för vars förhindrande det skulle ha fått användas sådant inhämtande av information genom vilket informationen har fåtts. Med brottsutredning avses att syftet med informationen är att använda den som stöd för bevis på skuld eller

som grund för ett avgörande om en metod för inhämtande av information (omedelbart utnyttjande) till åtskillnad till exempel från en avsikt att inrikta, där möjligheten att utnyttja överskottsinformationen är friare (indirekt utnyttjande). Vid begränsning som gäller användning av överskottsinformation som bevisning förbjuds utnyttjandet.

Enligt 5 kap. 54 § 2 mom. i polislagen får överskottsinformation dessutom alltid användas för förhindrande av brott, för inriktning av polisens verksamhet och som en utredning som stöder det att någon är oskyldig. Vad gäller förhindrande av brott måste man minnas att där även ingår avbrott av ett pågående brott. Informationen får däremot inte användas till att avslöja brott. Informationen kan alltid användas som bevis som stöd för att någon är oskyldig trots att detta i verkligheten kan bekräfta att någon annan är skyldig. I paragrafens 3 mom. föreskrivs att överskottsinformation också får användas för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada. Några ytterligare villkor har inte ställts för användningen av överskottsinformation i sådana situationer som det nu är tal om i 2 och 3 mom.

Överskottsinformation uppkommer i samband med alla slags åtgärder som hör till myndigheterna. Det är klart att också användningen av metoder för underrättelseinhämtning ofrånkomligen producerar annat än information som hotar den nationella säkerheten. I många fall bör denna information utplånas omedelbart med motiveringen att den är irrelevant, men en del av den information som är betydelselös för den nationella säkerheten kan gälla ett allvarligt brott. Därför behövs det lagstiftning för att styra att sådan information förs fram, förutom till relevanta mottagare av information överlag, speciellt även till förundersökningsmyndigheterna. En norm som placerar informationen på gränsytan till den civila underrättelseverksamheten och straffprocessen och utlämnandet av informationen där till förundersökningsmyndigheten vore komplex och principladdad. I ett skede som föregår fullbordandet av ett brott har målet att förhindra det företräde i förhållande till brottsutredningsintressen som preciserar förundersökningsfasen. Då är det frågan om åtgärder som å ena sidan är nödvändiga för att undvika fara och skada och som å andra sidan i regel inte kränker det centrala kärnområdet i individens rättssäkerhet. I domstolsskedet har man vanligtvis inte ansett det finnas något starkt konkurrerande intresse som motvikt till individens rättssäkerhet. I civil underrättelseverksamhet har å sin sida målet nationell säkerhet principiell prioritet i förhållande till intressena att förhindra och att utreda brott. I civil underrättelseverksamhet är det nämligen fråga om åtgärder som är nödvändiga för att försvara statens eller samhällets centrala intressen och trygga dem. Ett sådant intresse är rättssystemets, inklusive straffprocessystemets, funktionsduglighet. Därför passar inte 5 kap. 54 § i polislagen som sådan som förebild för regleringen av överlåtelse av information för brottsbekämpning, eftersom intresset att skydda den nationella säkerheten som hör till civil underrättelseverksamhet inte beaktas där.

Den första utgångspunkten för en bestämmelse om utlämnande av information för brottsbekämpning är att den bör innehålla anmälningsskyldighet till en förundersökningsmyndighet i sista hand om sådana brott för vilka det strängaste straffet är fängelse i sex år, för var och en har anmälningsskyldighet om så allvarliga brott som dessutom går att förhindra. Sådana gärningar har redan samband med ett så stort intresse att förhindra och utreda brott att det i fråga om dem inte är kriminalpolitiskt sett acceptabelt att inte lämna ut information till en förundersökningsmyndighet om brott i samband med civil underrättelseverksamhet, det vill säga en åtgärd genom vilken man kan undvika att en så allvarlig fara realiseras eller en skada uppkommer eller bidra till utredningen av ett grovt brott. Vidare vore det konsekvent att information som fåtts genom användning av en metod för underrättelseinhämtning alltid får överlämnas som en utredning till stöd för att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada. Dessa huvudsakligen individualistiska intressen har många likheter med de kollektiva intressen som den civila underrättelseverksamheten för sin del vill skydda. Med tanke på antagandet

om oskyldighet som tryggas i artikel 6.2 i Europeiska människorättskonventionen bör man emellertid undvika en lagstiftning som möjliggör utlämnande av information om alla, även ringa, brott till en förundersökningsmyndighet. Av samma skäl bör det även grundligt bedömas om information överlag kan ges till förundersökningsmyndigheter för kriminalunderrättelseinhämtning eller för inriktning av polisens verksamhet.

Underrättelse om informationsinhämtning

Frågorna om rättssäkerheten är på grund av den hemliga informationsinhämtningens karaktär utpräglat viktiga såväl för de parter som blir föremål för sådana åtgärder och för utomstående som för hela rättssystemets trovärdighet överlag. En av de viktigaste garantierna för rättsskyddet är att en part får bekanta sig med det material en myndighet innehar. Innan parten kan göra det måste den ha möjlighet att få information om användningen av hemlig informationsinhämtning. En parts rätt att få information är också en viktig förutsättning för en rättvis rättegång (21 § i grundlagen, artikel 6.1 i Europeiska människorättskonventionen och i artikel 14.1 i konventionen om medborgerliga och politiska rättigheter).

En i detta avseende fristående fråga gäller rätten att få information om en handling eller upptagning som tillkommit vid användning av en hemlig metod för inhämtande av information. I 11 § i lagen om offentlighet i myndigheternas verksamhet föreskrivs om en parts rätt att ta del av en handling. Enligt paragrafens 1 mom. är utgångspunkten den att en part har rätt att hos den myndighet som behandlar eller har behandlat ett ärende ta del också av en myndighetshandling som kan eller har kunnat påverka behandlingen, även om handlingen inte är offentlig. I paragrafens 2 mom. föreskrivs om sådana fall där en part eller dennes ombud eller biträde inte har sådan rätt som avses i 1 mom. Begränsningen gäller till exempel fall då utlämnande av uppgifter ur en handling skulle strida mot ett synnerligen viktigt allmänt eller enskilt intresse och fall där en handling har upprättats i samband med en förundersökning som ännu pågår, om utredningen skulle försvåras av att uppgifter lämnas ut.

Syftet med artikel 6.1 i Europeiska människorättskonventionen är bland annat att skydda parterna mot hemliga rättegångar. Jämlikheten mellan parterna, jämvikten och principen att parterna ska höras är viktiga principer när det gäller bedömningen av frågan om en rättegång som helhet betraktad ska anses vara rättvis. Principerna förutsätter att en part ska ha möjlighet att lägga fram sin sak under förhållanden som inte i sakligt hänseende försätter denne i en sämre situation än motparten. För att parterna ska vara jämlika krävs det att parterna behandlas likvärdigt och opartiskt i domstolen. Rätten att få information förutsätter även att en misstänkt har rätt till effektiv förberedelse av och motbevisning i sitt försvar. Å andra sidan måste det beaktas att jämviktsprincipen inte kränks av att något av rättegångsmaterialet fattas. Den situationen att en part har tillgång till eller känner till en omständighet som hemlighålls för en annan part måste bedömas på ett annat sätt. Dessutom måste man beakta principen att myndigheten inte i rättegångsskedet har rätt att bedöma betydelsen av en uppgift. Det är partens uttryckliga rätt.

Med tanke på antagandet om oskuld enligt artikel 6.2 i Europeiska människorättskonventionen kan det till exempel ha betydelse att informationskällor som handlar utifrån olika motiv inte vill eller kan ge objektiv information, eller åtminstone riktar in inhämtandet av information i enlighet med sina egna motiv. Om principen är att en informationskällas identitet eller att en informationskälla används överlag inte avslöjas kan informationskällans ansvar för informationens kvalitet eller användningen av den inte tillgodoses, utan myndigheten tar ansvaret.

Starka motiv för hemlighållande kan också föras fram. Sådana intressen är till exempel viktiga utredningsmässiga orsaker. Dessutom kan skydd av liv och hälsa, statens säkerhet samt skydd av sekretessbelagda taktiska och tekniska metoder förutsätta att meddelandet av information

skjuts upp eller att inhämtandet av information hemlighålls till och med helt. När det bestäms hur länge saken skjuts upp på grund av att brottsutredningen kan äventyras kan man tänka sig en tidsgräns, medan statens säkerhet samt behovet av skydd av liv och hälsa kan vara längre, och rentav permanent. Till exempel vad gäller täckoperationer avslöjar redan vetskapen om användningen av en metod i praktiken de tidigare operationer som gäller förhindrandet eller avslöjandet av brott som en person deltagit i och leder till att personen inte kan användas i framtiden. Dessutom kan vetskapen i värsta fall äventyra personens och hans eller hennes närståendes liv och hälsa. Om man i samma ärende har anlitat en informationskälla och en person under täckmantel räcker det att redan en av dessa avslöjas för att båda personernas och deras närståendes liv och hälsa ska vara i fara.

Europadomstolen har bland annat i sina avgöranden Rowe och Davis mot Förenade kungariket 16.2.2000, Natunen mot Finland 31.3.2009, Janatuinen mot Finland 8.12.2009, Bannikova mot Ryssland 4.11.2010 och Bulfinsky mot Rumänien 1.6.2010 godkänt att allt material inte avslöjas för den misstänkte om det motsatta intresset gäller nationell säkerhet, skydd av liv och hälsa eller sekretessbelagda utredningsmetoder. Artikel 6.1 i Europeiska människorättskonventionen tillåter dock endast ovillkorligen nödvändiga ingrepp i en åtalads rättigheter.

Polislagens 5 kap. 58 § 1 mom. gäller teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, systematisk observation, förtäckt inhämtande av information, teknisk observation och kontrollerade leveranser. Föremålet för metoderna som används ska utan dröjsmål underrättas skriftligen efter att syftet med informationsinhämtningen har uppnåtts. Den ovillkorliga tidsfristen i 1 mom. är dock ett år efter att informationsinhämtningen har upphört. Därefter ska föremålet underrättas om saken. Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om underrättelsen. Momentet gäller inte inhämtande av basstationsuppgifter, observation och identifieringsuppgifter för teleadresser eller teleterminalutrustning. Underrättelsen ska specificeras med sådan noggrannhet att föremålet för informationsinhämtningen vid behov kan försöka utreda grunderna för användningen av metoderna. I underrättelsen ska det nämnas vilken metod som använts samt var och när den använts. Sekretessbelagda taktiska och tekniska metoder behöver inte avslöjas i underrättelsen. Om föremålets identitet förblir oklar kan underrättelsen naturligtvis inte göras. Om föremålets identitet klarnar senare ska personen underrättas i efterhand. Trots att hemliga metoder för inhämtande av information i verkligheten även riktas mot andra personer behöver de inte underrättas.

Polislagens 5 kap. 58 § 3 mom. gäller systematisk observation, förtäckt inhämtande av information, täckoperationer, bevisprovokation genom köp och styrd användning av informationskällor. Huvudregeln är att föremålet för informationsinhämtningen ska underrättas om metoderna om en förundersökning inleds i ärendet. Om en förundersökning inleds, ska bestämmelserna i 10 kap. 60 § i tvångsmedelslagen iakttas i tillämpliga delar. Samtidigt ska den domstol som beviljat tillståndet och, ifråga om täckoperationer, den domstol som avses i 32 §, det vill säga Helsingfors tingsrätt, informeras skriftligen om underrättelsen. Samma sak gäller bevisprovokation genom köp och användning av styrda informationskällor med stöd av 10 kap. 60 § 7 mom. i tvångsmedelslagen och med iakttagande av bestämmelserna i 43 § 6 mom. i samma kapitel i tillämpliga delar. Det måste beaktas att domstolen spelar en roll i beslutsfattandeprocessen endast i fråga om täckoperationer. Så är det inte vid bevisprovokation genom köp och användning av styrda informationskällor. Trots detta ska domstolen ges skriftlig information om underrättelsen till föremålet om alla dessa medel.

Polislagens 5 kap. 58 § 2 mom. innehåller å sin sida undantag från huvudregeln om underrättelser. Enligt momentet kan domstolen på yrkande av en anhållningsberättigad polisman besluta att underrättelsen enligt 1 mom. till den som varit föremål för åtgärden får skjutas upp med högst två år åt gången, om det är motiverat för att trygga pågående inhämtande av in-

formation, trygga statens säkerhet eller skydda liv eller hälsa. Grunden som gäller statens säkerhet kommer i praktiken i fråga endast på skyddspolisens verksamhetsområde. Det ska beaktas att beslutet om att skjuta upp underrättelsen inte förpliktar till att dröja med underrättelsen till den utsatta dagen. Om förhållandena ändras så att det inte längre finns förutsättningar för att inte lämna en underrättelse ska den göras oberoende av beslutet om uppskov (biträdande justitieombudsmannens avgöranden Dnr 1716/2/09 och Dnr 609/2/10). Grunderna för uppskjutande täcker också fall som gäller olika internationella gemensamma operationer liksom fall där det upptäcks att föremålet för informationsinhämtning varit oriktigt. Att skjuta upp innebär alltså att flytta fram underrättelsen, men det är även möjligt att helt låta bli att underrätta. Det kan enligt det ovan nämnda momentet göras om det är nödvändigt för att trygga statens säkerhet eller skydda liv eller hälsa. Domstolen beslutar om uppskjutandet av underrättelsen eller om att underrättelsen ska utebli trots att en anhållningsberättigad tjänsteman har beslutat om användningen av metoden.

Bestämmelsen om underrättelse om användning av hemliga metoder för inhämtande av information i 5 kap. 58 § i polislagen är till sina grundläggande lösningar ändamålsenlig också vad gäller underrättelse om användningen av metoderna i 5 a kap. i polislagen. Eftersom det med civil underrättelseverksamhet avses informationsinhämtning som skyddspolisen utför bör det anges att den som framför en begäran om att en underrättelse ska skjutas upp eller utebli ska vara en polisman som hör till skyddspolisens befäl. Det finns skäl för att låta domstolen avgöra om en underrättelse ska skjutas upp eller få utebli helt, eftersom olika parters rättigheter och behov av information bäst kan bedömas på detta sätt. Med beaktande av att bestämmelserna i polislagens 5 a kap. bygger på informationsinhämtning om verksamhet som hotar den nationella säkerheten bör tryggandet av den nationella säkerheten läggas till i grunderna för att en underrättelse ska skjutas upp eller utebli. Dessutom bör det bedömas hur underrättandet ska ordnas såväl med tanke på föremålets rättsskydd som på det lämpligaste sättet i fråga om de praktiska möjligheterna att underrätta om de nya metoder som föreslås i polislagens 5 a kap., det vill säga platsspecifik underrättelseinhämtning och kopiering samt underrättelseinhämtning som avser datatrafik i en separat lag som föreslås. Om föremålet för underrättelseinhämtning är en främmande stats myndighet eller en person som agerar för en främmande stats räkning finns det ingen skyldighet att underrätta om användning av metoder för informationsinhämtning.

Tvångsmedel som skyddspolisen använder

Genomsökning

Polislagen innehåller i nuläget inga bestämmelser om platsgenomsökning eller husrannsakan i syfte att inhämta information. I 8 kap. i tvångsmedelslagen föreskrivs det däremot om platsgenomsökning som utförs för brottsutredning. Genomsökningarna enligt den gällande tvångsmedelslagen utförs med vetskap av eller i närvaro av den som är föremål för åtgärden med syftet att skaffa bevis för ett brott. Det är dock motiverat att beakta att det i tvångsmedelslagen för närvarande inte finns bestämmelser om genomsökning med syftet att hämta information utan att föremålet för informationsinhämtning vet om det, och därför betyder termen ”genomsökning” som används i detta sammanhang inte samma sak som genomsökning i den gällande tvångsmedelslagen.

I underrättelseverksamheten uppstår det situationer där det är nödvändigt att verkställa genomsökning av en plats för att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten. Hur lång tid informationsinhämtningen ska ta ska inte bestämmas i förväg, utan det beror på hurdan och vilken typ av information skyddspolisen kan inhämta genom sina lagstadgade befogenheter. Om skyddspolisens informationsinhämtning avslöjas för den som är föremål för inhämtningen kan detta äventyra förverkligandet av syftet med den civila

underrättelseverksamheten och kan orsaka fara för liv eller hälsa för tjänstemannen vid skyddspolisen.

Föremålet kan ändra på sina rutiner för att undanhålla dem för underrättelsemyndigheten, skrida till andra motåtgärder som riktas mot myndigheterna eller varna potentiella övriga föremål för underrättelseinhämtning att han eller hon är föremål för sådan. Därför kan skyddspolisens anmälningsplikt, om den aktualiseras i ett för tidigt skede, omintetgöra hela planen där insamlandet av information bedrivs.

Samhällets intresse är större ju allvarligare projekt eller fenomen det är fråga om. Utgångspunkten är att all verksamhet som hotar den nationella säkerheten på grund av sin skadlighet är sådan att det bör gå att inhämta så omfattande information som möjligt.

Till exempel en terroristgrupps verksamhet är till karaktären systematisk, strävar systematiskt efter ett brottsligt mål och är kollektiv. En följd av kollektiviteten är att delåtgärderna som är nödvändiga för att möjliggöra terroristiska projekt delas så att de utförs av flera medlemmar. Då kan inhämtandet av information om hela verksamhetshelheten visa sig vara mycket utmanande. Med hjälp av cell- eller nätverksliknande organisationsformer strävar man efter att minimera gruppens synlighet och hemlighålla planerna så effektivt som möjligt utöver de traditionella kommunikationsmöjligheterna. Man strävar ofta efter att minimera kontakten mellan gruppmedlemmarna eller göra kommunikationens innehåll så svårt att tolka som möjligt för utomstående. De tekniska krypteringsmöjligheter och anonymitetsskyddet som den moderna kommunikationstekniken tillåter utnyttjas effektivt. Alla ovan nämnda faktorer bidrar till att skyddspolisens metoder för inhämtande av information inte alltid producerar information med vars hjälp brott kan förhindras i förväg eller avslöjas.

Trots det ovan relaterade är det ett faktum att terroristisk verksamhet kräver fysiska aktiviteter i den reella världen. Sådana aktiviteter lämnar i allmänhet olika spår av olika grader. Spåren kan till exempel vara utkast, dokument som visar gruppens interna arbetsfördelning, anteckningar som gäller underrättelseinhämtning om eller bevakning på förhand av ett planerat mål för attacker, resedokument, e-postmeddelanden som har samband med en plan och som öppnats med ett krypteringsprogram i en dator eller ämnen eller föremål som behövs för att genomföra en plan. I vissa fall kan man få information om ovan nämnda eller liknande omständigheter som dem genom en genomsökning till exempel i ett utrymme som en person eller en grupp använder som samlingslokal eller som lager. Genomsökningen kan producera information som kan antas ha en mycket viktig betydelse för verksamhet som allvarligt hotar den nationella säkerheten.

Det finns ingen orsak att underrätta föremålet för en sådan åtgärd om att genomsökning verkställs, eftersom det kan vara nödvändigt att fortsätta informationsinhämtningen om verksamheten ännu efter genomsökningen. En anmälningsplikt som är bunden till ögonblicket för genomsökningen omintetgör framtida framgångsrik informationsinhämtning. Det kan till exempel bero på att genomsökningen har verkställts vid fel tidpunkt. Man kan tänka sig en situation där skyddspolisen får information som kan anses tillförlitlig om att en okänd aktör ska träffa föremålet och leverera en viktig plan till denne. Skyddspolisen har kännedom om leveransen men inte om den exakta tidpunkten. Om skyddspolisen företar en genomsökning i ett utrymme som personen förvaltar innan mötet är över fungerar en underrättelse till föremålet om genomsökningen som en varning som får personen att ändra planen för sin verksamhet. För att säkerställa en helhetsbild kan man bli tvungen att genomföra genomsökning på olika föremål samtidigt. Då får information om genomsökningen inte komma till eventuella övriga partners kännedom.

Informationsinhämtningens effektivitet grundar sig på så sätt på att föremålet åtminstone inte omedelbart blir medvetet om de åtgärder som riktas mot honom eller henne. Det är snarare fråga om hemlig informationsinhämtning än om genomsökning enligt tvångsmedelslagen. I regel bör föremålet emellertid i ett senare skede underrättas om åtgärden. Underrättelsen bör göras efter att syftet med inhämtandet av information har uppnåtts. Anmälningsplikten kan emellertid skjutas upp eller man kan avstå från den om synnerligen viktiga intressen motiverar detta från fall till fall. Det är befogat att ställa villkoren för uppskjutandet av eller avståendet från anmälningsplikten på samma nivå som i fråga om hemliga metoder för inhämtande av information enligt 5 kap. i polislagen. Genomsökning kan i detta sammanhang kallas platsspecifik underrättelseinhämtning.

Kopiering

I civil underrättelseverksamhet är det under platsspecifik underrättelseinhämtning och även annars nödvändigt att ta hand om observationer och fynd. I princip bör det vara möjligt att kopiera föremål, egendom, dokument, information eller omständigheter som hittats vid platsspecifik underrättelseinhämtning. För verkställandet av platsspecifik underrättelseinhämtning behövs det bestämmelser om motsvarande kopiering som metod för underrättelseinhämtning i polislagens 5 a kap. som anges om metoden i tvångsmedelslagen. Kopiering bör antecknas i protokollet om genomsökning av plats, och dessutom bör ett eget protokoll upprättas över var och en av dem. Personen som är föremål för kopieringen eller den vars egendom, föremål eller dokument det är fråga bör dessutom underrättas på samma sätt som det ska bestämmas om underrättelse om metoder för underrättelseinhämtning.

Eftersom utgångspunkten är att det är meningen att civil underrättelseverksamhet och de metoder för underrättelseinhämtning som används där ska hållas hemliga för föremålet för dem kommer inte heller omhändertagande av dokument, föremål eller egendom som tillhör personen heller på frågan. Därför är kopiering en nödvändig metod för att man ska kunna undvika att ta om hand de observationer och fynd som gjorts och samtidigt minimeras risken att avslöjas, såsom till exempel att en operation för underrättelseinhämtning avslöjas i samband med platsspecifik underrättelseinhämtning. Om man i civil underrättelseverksamhet, till exempel i platsspecifik underrättelseinhämtning, hittar farliga föremål eller ämnen kan man förfara enligt 2 kap. 14 och 15 § i polislagen. Till denna del är det även motiverat att beakta att om man i ett utrymme som är föremål för platsspecifik underrättelseinhämtning hittar farliga föremål eller ämnen och om de eventuellt också bytts ut mot ofarliga har tröskeln för ett brott eller något annat ”skäl att misstänka” ett brott enligt strafflagen som ska förhindras eller avslöjas högst sannolikt överskridits. Då övergår man från användningen av metoder för underrättelseinhämtning till befogenheter till följd av brott och ärendet överförs till centralkriminalpolisen med vissa undantag.

När man vid platsspecifik underrättelseinhämtning till exempel tar bilder av dokument som hittas i utrymmet som är föremål för åtgärden utförs samtidigt kopiering av dokumentet. Under platsspecifik underrättelseinhämtning eller genast efter den är det inte nödvändigtvis klart vilken betydelse dokumenten har, och utredningen av innehållet i dem kan till exempel kräva att de översätts. Vid kopiering måste man emellertid beakta föremålet för den. Om föremålet för kopiering är ett dokument som innehåller kommunikation mellan personer bör förutsättningarna för att använda kopiering vara högre än vid kopiering av meddelanden som inte åtnjuter konfidentiellt skydd.

Underrättelseinhämtning som avser utländska förhållanden

Bakgrunden till de ändringar som skett i skyddspolisens verksamhetsbetingelser de senaste åren är att hoten mot den inre och den nationella säkerheten och fenomen som har samband

med dem allt snabbare internationaliseras och blir mer datatekniska. Gränserna mellan inre och yttre säkerhet har fördunklats och den inre säkerhetens yttre dimension har accentuerats. Den nationella och den internationella verksamhetsmiljön sammanlänkas allt tätare. De allvarligaste hoten mot Finlands nationella säkerhet är nästan utan undantag av internationellt ursprung eller har kopplingar utomlands. Därför finns all information som påverkar det finländska samhället inte tillgänglig på finländskt territorium. En enskild stat förmår inte i alla situationer avvärja hot som riktas mot den med enbart egna åtgärder. Förändringen betonar internationellt underrättelse- och säkerhetsarbete samt betydelsen av den operativa och strategiska information som fås den vägen. Verksamhetsområdets operativa och strategiska internationella kommunikation har nästan fyrdubblats på 2000-talet.

Om man vill skydda samhället framgångsrikt måste de finländska säkerhetsmyndigheterna kunna inhämta information även från utländska aktörer. Med underrättelseinhämtning som avser utländska förhållanden avses inhämtande av information om utländska förhållanden och föremål som är väsentlig med tanke på den nationella säkerheten. Syftet med underrättelseinhämtning som avser utländska förhållanden är att producera information som är nödvändig för den högsta statsledningens säkerhetspolitiska beslutsfattande samt för att avvärja allvarliga yttre hot mot säkerheten.

Utgångspunkten för underrättelseinhämtning som avser utländska förhållanden är på grund av dess karaktär att man strävar efter den information som behövs med så lätta metoder som möjligt. I praktiken grundar sig underrättelseinhämtningen ofta på handlingsmodeller som nära påminner om förbindelseverksamhet. Det är fråga om utbyte av information och synpunkter mellan två stater som grundar sig på frivillighet mellan myndigheter och som gynnar båda parterna. Informationsutbytet kan till exempel gälla fenomen, enskilda händelser, observationer eller politiska stämningar som är föremål för ett gemensamt intresse, och om vilka parten som ger information genom sin tolkning försöker påverka mottagarens uppfattningar. Vid sidan av sådant ömsesidigt informationsutbyte kan underrättelseinhämtningen som avser utländska förhållanden baseras på ensidig verksamhet av den ena staten. I utgångssituationen består verksamhetens innehåll av att personal som sänts utomlands av staten som inhämtar information med stöd av sin tjänsteställning gör allmänna observationer om förhållandena i staten där de är stationerade samt diskuterar med representanter för den staten eller med medborgare. Trots att det då inte är fråga om informationsutbyte som uttryckligen har avtalats med staten där de är stationerade sker verksamheten ofta med den statens tysta godkännande. Alla stater blir de facto till en viss gräns tvungna att tolerera att underrättelseinhämtning sker på deras mark.

Under vissa förhållanden som kan karaktäriseras som exceptionella är sådan underrättelseinhämtning som beskrivs ovan och som betonar samarbete eller tyst godkännande inte längre tillräcklig. Med tanke på Finlands nationella säkerhet måste man i sådana fall kunna inhämta kritiskt sett viktiga uppgifter med hjälp av hemliga metoder för underrättelseinhämtning.

De flesta europeiska stater har reglerat sin underrättelseverksamhet som avser utländska förhållanden och de befogenheter som ska användas där. Det varierar från land till land hur noggrant man ansett det relevant att reglera enskilda befogenheter. Med underrättelseinhämtning som avser utländska förhållanden avses aktiv verksamhet av säkerhetsmyndigheter för att inhämta information om sådana enskilda eller statliga aktörer som vistas utomlands och som kan hota Finlands nationella säkerhet eller andra intressen som är livsviktiga för samhället.

Perspektivet för den stat som blir föremål för verksamheten

Enligt en allmän princip inom internationell rätt åtnjuter varje suverän stat territoriell integritet och politiskt oberoende i förhållande till andra stater. Varje stat beslutar själv om och på vilka villkor den tillåter utländska tjänstemäns verksamhet på sitt territorium. De flesta stater tolere-

rar till en viss gräns eller rentav godkänner de facto verksamheten hos främmande myndigheter för underrättelseinhämtning på sin mark. Det kan vara fråga om informationsutbyte som gynnar båda parterna eller om att det datainsamlande som den främmande makten öppet verkställer om allmänna förhållanden inte äventyrar statens eller någon annan parts intressen. Under andra förhållanden kan staten som är föremålet förhålla sig avvisande till verksamhet från främmande staters myndigheter på dess territorium. Verksamheten kan från fall till fall även uppfylla rekvisitet för någon gärning som är straffbar enligt den statens strafflag. Verksamhetens straffbarhet kan beroende på staten som är föremål för den påverkas till exempel av vem som inhämtar informationen, vilken information som inhämtas och den metod som används. Staterna som jämförs har inte heller på lagnivå ställt som villkor för ett utlands underrättelseinhämtning att staten godkänner verksamheten eller att denna inte bryter mot statens gällande lagar.

I underrättelseinhämtning som avser utländska förhållanden är det fråga om ett acceptabelt mål, det vill säga verksamhet som krävs för att uppnå skyddet av den nationella säkerheten, som i vissa fall kan innebära risker. En av riskerna är att det är fråga om verksamhet som strider mot lagstiftningen i staten eller som den på annat sätt inte anser vara godtagbar. I underrättelseinhämtning som avser utländska förhållanden är det viktigt att beakta hur de andra staterna förhåller sig och innehållet i deras lagstiftning men av praktiska skäl kan detta inte beaktas när verksamheten regleras utan först när den påbörjas. Då gäller det att överväga om intresset som verksamheten ger den nationella säkerheten är klart större än de risker som ingår där.

Tredje staters synvinkel

Enligt en allmän princip inom internationell rätt åtnjuter varje suverän stat territoriell integritet och politiskt oberoende i förhållande till andra stater. Detta gäller också när underrättelseinhämtningen sker genom att på något sätt utnyttja en tredje stats territorium. Dessutom får enligt en allmän princip i internationell rätt en stat inte tillåta att dess territorium används för gärningar som påverkar andra stater på ett skadligt och illegalt sätt. När gärningen bedöms tillmäts den inte betydelse enbart i fråga om huruvida den orsakar skada på egendom eller personer, utan det kan vara tillräckligt att den överlag ger upphov till negativa konsekvenser. I underrättelseinhämtning som avser utländska förhållanden kan till exempel personer som fungerar som informationskällor påträffas på en tredje stats territorium eller sådana kan värvas där. Principen om transitland kan dock inte anses gå att tillämpa direkt på internationell datatrafik där datatrafik normalt sett rör sig och dirigeras på ett sätt som inte fastställs på förhand där det inte finns några hinder för den.

Underrättelseverksamhet och internationell rätt

Enligt artikel 38 i internationella domstolens stadga är de viktigaste källorna för internationell rätt allmänna eller speciella internationella överenskommelser, internationell sedvänja och så kallade allmänna rättsgrundsatser. Inga internationella fördrag har upprättats om underrättelseverksamhet i fredstid. Bestämmelserna om skydd som spioner åtnjuter under krig i artikel 46 i första tilläggsprotokollet till Genèvekonventionen 1949 har å sin sida ingen betydelse för det ämne som behandlas här.

Trots att underrättelseverksamheten i princip gäller kränkning av den stats suveränitet som är föremål för verksamheten råder det inte enighet i rättslitteraturen om huruvida den internationella rätten på nivån för sedvänja och allmänna rättsprinciper godkänner eller fördömer underrättelseverksamhet. Underrättelseverksamhet kan inte anses ha en allmänt accepterad internationellt rättslig ställning eftersom stater genom att förklara en person som persona non grata eller på annat sätt icke acceptabel upprepade gånger visar att de inte godkänner sådan aktivitet. Å andra sidan kan underrättelseverksamhet inte heller internationellt rättsligt sett an-

ses förbjuden eftersom nästan alla stater bedriver denna verksamhet. Det är fråga om globalt etablerad verksamhet, och enskilda staters attityd till den beror på om de i respektive fall har rollen som stat som inhämtar underrättelser eller är föremål för den.

Trots att underrättelseverksamheten inte är reglerad visar flera internationella exempel att man i verksamheten har utnyttjat möjligheterna i det internationella traktaträttssystemet. I verksamheten har man använt sig av en representants diplomatiska immunitet och frihet från den straffrättsliga domsrätten i staten som är föremål för verksamheten som garanteras i Wienkonventionen (FördrS 3–5/1970) om diplomatiska förhållanden.

Skyddspolisens informationsinhämtning utomlands

De finländska säkerhetsmyndigheterna har inga reglerade befogenheter att inhämta information utomlands. Beroende på den ändrade säkerhetsmiljön och på de grunder som nämns i denna proposition behövs det emellertid bestämmelser om befogenheter utomlands, det vill säga underrättelseinhämtning som avser utländska förhållanden. Det föreslås att befogenheterna utomlands för den civila verksamhetens del ska ges till skyddspolisen och att de metoder som föreslås i 5 a kap. i polislagen som föreslås används i underrättelseinhämtning som avser utländska förhållanden. Det ska regleras separat om internationellt samarbete och om metoder för underrättelseinhämtning i samband med det.

I internationell jämförelse kan det noteras att beslutsfattandet om informationsinhämtning utomlands varierar från land till land. Till exempel en underrättelsemyndighet själv eller någon aktör med politiskt ansvar kan ansvara för beslutsfattandet. Om en underrättelsemyndighet ansvarar för beslutsfattandet sker det i allmänhet inom ramen för riktlinjer från statsledningen. Metoderna som används inom underrättelseinhämtningen riktas mot suveräniteten i en främmande stat som är föremål för verksamheten och eventuellt också i en tredje stat genom vilken informationsinhämtningen sker. Därför accentueras den politiska dimensionen i underrättelseinhämtning som avser utländska förhållanden. Underrättelseinhämtningens eventuella konsekvenser och risker påverkar beslutsprocessen. Chefen för skyddspolisen beslutar alltid om civil underrättelseverksamhet utomlands och om användningen av metod för underrättelseinhämtningen. Finländska domstolar har inte behörighet att besluta om användning av metoder utanför Finlands territorium och kommer därför inte på fråga som beslutsfattare. Dessutom är det på grund av utrikespolitiska känsligheter i underrättelseinhämtning som avser utländska förhållanden motiverat att risken vid användningen av metoder bärs av den som genomför denna underrättelseinhämtning, det vill säga skyddspolisen. Det regleras separat om samordningen av civil och militär underrättelseverksamhet. De utrikespolitiska dimensionerna i underrättelseinhämtningen som avser utländska förhållanden behandlas på så sätt även i samband med att civil och militär underrättelseverksamhet samordnas då de centrala utrikespolitiska myndigheterna deltar.

Det ska regleras separat om internationellt samarbete och även då är det chefen för skyddspolisen som beslutar om metoder för underrättelseinhämtning i en operation som genomförs utomlands. Skillnaden mellan internationellt samarbete och underrättelseinhämtning som avser utländska förhållanden ligger i om den stat som är föremål är medveten om operationen. Underrättelseinhämtning som avser utländska förhållanden utförs i princip utan att staten som är föremål för den eller en tredje stat vet om det medan internationellt samarbete grundar sig på att staten som är föremål för det ger sitt samtycke, eller alternativt i samråd med en tredje stat utan att staten som är föremål vet om det.

Internationellt samarbete

Polisen ska upprätthålla säkerheten i samarbete med andra myndigheter samt med sammanslutningar och invånarna och sköta det internationella samarbete som hör till dess uppgifter. Polisens internationella samarbete regleras i 9 kap. 9 § i polislagen. För polisens del möjliggör den gällande nationella lagstiftningen rättslig hjälp och handräckning till polisen i en främmande stat och på motsvarande sätt rättslig hjälp och handräckning från en främmande stat till polisen om det finns separata bestämmelser eller avtal om det. På motsvarande sätt gäller det som separat föreskrivs om saken eller det som avtalats i ett internationellt fördrag som är förpliktande för Finland i fråga om en främmande stats polismans rätt att använda befogenheten för en finländsk polisman. I internationellt samarbete som skyddspolisen gör med säkerhets- och underrättelsetjänster iakttas dock inte bestämmelserna om polisens rättsliga hjälp och handräckning.

Till skyddspolisens arbete som gäller nationell säkerhet hör i väsentlig grad samarbete med andra länders säkerhets- och underrättelsetjänster. Till samarbetet hör bland annat konfidentiellt informationsutbyte om olika hot mot säkerheten. Det existerar inga multilaterala och för Finlands del inte heller bilaterala internationella fördrag om internationellt samarbete i fråga om underrättelseinhämtning. Vad gäller samarbete och utbyte av underrättelseinformation har emellertid internationella etablerade förfaringssätt utformats under årens lopp. Information som utbyts mellan skyddspolisen och utländska säkerhets- och underrättelsemyndigheter gäller en fras om ändamålsbundenhet som grundar sig på internationell etablerad sedvänja som förhindrar att information utlämnas till tredje part utan uttryckligt samtycke från landet som de utlämnas från. Också skyddspolisen är i sin internationella verksamhet tvungen att följa denna avtalade fras. Förutom utbyte av information består internationellt samarbete även av till exempel tekniskt stöd, utbildning, utbyte av tjänstemän och verksamhet med internationella kontaktpersoner.

Den gällande polislagen har inga bestämmelser om samarbete mellan internationella säkerhets- och underrättelsetjänster. Därför behöver det göras möjligt att genomföra internationella gemensamma operationer inom civil underrättelseverksamhet så, att en polisman från skyddspolisen kan delta i sådana utomlands och en tjänsteman inom säkerhets- eller underrättelsetjänsten i en främmande stat kan delta i en sådan på finländskt territorium genom att detta bestäms i lagen.

Juridisk tillsyn över skyddspolisen

Polisens hemliga metoder för inhämtande av information övervakas enligt 5 kap. 63 § 1 mom. i polislagen av cheferna för de enheter som använder hemliga metoder för inhämtande av information, samt dessutom av inrikesministeriet när det är fråga om skyddspolisen och av Polisstyrelsen när det är fråga om en enhet som är underställd Polisstyrelsen. Inrikesministeriet ska enligt 2 mom. årligen till riksdagens justitieombudsman avge en berättelse om hur hemliga metoder för inhämtande av information och skyddandet av dem har använts och övervakats. I 10 kap. 65 § i tvångsmedelslagen finns motsvarande bestämmelser om användning av hemliga tvångsmedel.

I statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information finns det också bestämmelser om registrering av hemliga metoder för inhämtande av information, övervakning och redogörelser för metoder för inhämtande av information. Dessutom har myndigheterna interna föreskrifter om inhämtandet av information.

Riksdagens justitieombudsmans övervakning av hemliga metoder för inhämtande av information baseras huvudsakligen på inspektioner och övrig tillsyn på eget initiativ. Endast ett fåtal

klagomål görs årligen om användning av hemliga metoder för inhämtande av information. Justitieombudsmannen ger för varje år riksdagen en berättelse om sin verksamhet samt om rättskipningens tillstånd och om brister som han eller hon upptäckt i lagstiftningen. Grundlagsutskottet har krävt att berättelsen får ett eget avsnitt om teletvångsmedel och täckoperationer (GrUB 15/2002 rd).

Grundlagsutskottet har flera gånger (GrUB 8/2007 rd, GrUB 17/2006 rd och GrUB 16/2006 rd) å ena sidan konstaterat att justitieombudsmannen spelar en viktig roll när det gäller att övervaka teletvångsmedlen och utveckla övervakningssystemen. Men justitieombudsmannens laglighetsövervakning kan enligt utskottet å andra sidan bara utgöra ett komplement till de förvaltningsinterna övervakningsmekanismerna. Utskottet har dessutom i ett annat sammanhang konstaterat att man måste se till att rättstryggheten i anknytning till teletvångsmedel, i synnerhet domstolarnas tillståndsförfarande, den interna myndighetsövervakningen och justitieombudsmannens laglighetskontroll fungerar såväl på författningsnivå som i praktiken (GrUU 32/2013 rd).

Också justitieombudsmannen har i berättelsen för 2014 bedömt att de årliga rapporterna som fås av myndigheterna förbättrar möjligheterna att på ett allmänt plan följa upp användningen av hemligt inhämtande av information. Justitieombudsmannens särskilda övervakning i konkreta enskilda fall kan emellertid endast vara stickprovsmässig. I berättelsen noteras det att justitieombudsmannens övervakning i första hand endast kan ses som ett komplement till myndigheternas interna laglighetskontroll, och den kan karaktäriseras som kontroll av kontrollen.

Behandling av personuppgifter

I den gällande lagen om behandling av personuppgifter i polisens verksamhet finns bestämmelser förutom om skyddspolisens funktionella informationssystem också om användningen av personuppgifter i de syften som anges i 1 kap. 1 § i polislagen samt om informationsutbyte med andra polisenheter, med andra myndigheter samt med andra staters behöriga myndigheter. Informationsutbytet regleras även i andra lagar. Däremot regleras inte befogenheter i polisens personuppgiftslag. Till exempel ska rätten att få information oberoende av skyddspolisens sekretessbestämmelser samt rätten och skyldigheten att utlämna information även i fortsättningen regleras i polislagen.

I denna proposition föreslås det att skyddspolisens befogenheter ändras. Det föreslås likaså att skyddspolisens uppgift i polisförvaltningslagen ändras så att den omfattar inhämtande av information också för att skydda den nationella säkerheten. Det föreslås också att 1 kap. 1 § 1 mom. i polislagen ändras så att det blir polisens uppgift att skydda den nationella säkerheten. Skyddspolisens lagstadgade uppgift omfattar med ändringarna även i fortsättningen aktiv övervakning av Finlands säkerhetsmiljö, inhämtande av information som gäller att förutse hot mot säkerheten och analys av informationen. Informationen inhämtas och fås till exempel ur öppna källor eller av andra myndigheter genom rätt att få information som det föreskrivs om separat. Skyddspolisen inhämtar således information i större utsträckning än enbart för att utföra uppdrag genom de hemliga metoder för inhämtande av information som reglerats eller genom de nya befogenheter för underrättelseinhämtning som föreslås i denna proposition.

Inrikesministeriet tillsatte den 28 januari 2016 ett lagstiftningsprojekt med syftet att reformera lagstiftningen om polisens behandling av personuppgifter. Avsikten är att totalrevideringen av polisens personuppgiftslag ska träda i kraft under 2019. Eftersom man genom de nya befogenheterna för underrättelseinhämtning vid sidan av övriga uppgifter även får personuppgifter, och eftersom dessa befogenheter eventuellt regleras så att de träder i kraft redan innan polisens personuppgiftslag som ska reformeras föreslås det att polisens personuppgiftslag som nu är i kraft ändras. I detta sammanhang har man inte upptäckt betydande behov av ändringar i den

gällande personuppgiftslagen för polisen. Det föreslås att endast 5 § i polisens personuppgiftslag som gäller skyddspolisens funktionella informationssystem, polisens rätt att få uppgifter ur vissa register och informationssystem i 13 § samt rätten till insyn i 45 § ska ändras.

Skyddspolisen ska för att fullgöra sin uppgift upprätthålla skyddspolisens funktionella informationssystem. Skyddspolisen registrerar inte personuppgifter som den behöver för sitt uppdrag i andra register. Därför föreslås det att också de personuppgifter som fås med de nya befogenheterna registreras i detta system. Det föreslås att lagen ändras så att personuppgifter som skyddspolisen måste behandla för att kunna skydda den nationella säkerheten och för att förhindra, avslöja och utreda förehavanden eller brott som äventyrar rätts- och samhällsordningen eller statens säkerhet kan registreras i informationssystemet.

Då kan personuppgifter som skyddspolisen behöver för att fullgöra sin lagstadgade uppgift registreras i systemet. Skyddspolisens uppgift fastställs även i fortsättningen ingående och den består också av annat än de befogenheter som anges för den. Att trygga statens säkerhet och att skydda den nationella säkerheten är inte synonyma, men båda används redan i den gällande lagstiftningen och de avses som begrepp i praktiken i stort sett betyda samma sak. I detta sammanhang beskrivs skyddspolisens uppdrag med båda termerna. Därför avses med skyddandet av den nationella säkerheten och tryggandet av statens säkerhet i praktiken samma sak som i polisens personuppgiftslag och samma sak som anges om skyddspolisens uppgift. Med skyddet av den nationella säkerheten eller tryggandet av statens säkerhet avses uppgiften att upprätthålla rätts- och samhällsordningen så att allmänhetens grundtrygghet och samhällets funktioner tryggas. Personuppgifter kan därför behandlas på samma sätt som det föreskrivs såväl om den nationella säkerheten som om statens säkerhet. Eftersom dessa begrepp kan anses innebära samma sak i polisens personuppgiftslag föreslås det inte i detta sammanhang att begreppen förenhetligas i hela den lagen. I totalrevideringen av polisens personuppgiftslag är avsikten däremot att förenhetliga begreppen och således använda endast begreppet nationell säkerhet i situationer där det till exempel inte är nödvändigt att separat nämna alla skyddspolisens uppgifter.

För skyddspolisens uppgift och hanteringen av personuppgifter som hör dit är det viktigt att personuppgifter som erhållits via olika befogenheter kan behandlas på samma sätt och i samma register hos skyddspolisen och att det inte finns olika grader av trösklar för utlämnande av dem beroende på vilket sätt de erhållits. För att fullgöra skyddspolisens uppgifter behandlas personuppgifter antingen på det sätt som användningsändamålet förutsätter eller avvikande från det för att trygga statens säkerhet eller skydda den nationella säkerheten.

Befogenheter för förundersökning

Inom polisförvaltningen ansvarar skyddspolisen för att förhindra, avslöja och även utreda brott som avses i strafflagens 12 kap. (landsförräderibrott) och 13 kap. (högförräderibrott). Skyddspolisen ansvarar också för förundersökningen av brott som avses i strafflagens 17 kap. 1 § (offentlig uppmaning till brott), 15 kap. 10 § 1 mom. (underlåtenhet att anmäla grovt brott) och 15 kap. 11 § (skyddande av brottsling) om brottet har samband med landsförräderi- eller högförräderibrott.

I fråga om terroristbrott i strafflagen 34 a kap. är det skyddspolisens uppgift att förhindra och avslöja dem. Förundersökningen av terroristbrott verkställs i en polisenhet som underlyder Polisstyrelsen som skyddspolisen samarbetar med och vid behov bistår i förundersökningen. Skyddspolisen kan av särskilda skäl som grundar sig på statens säkerhet verkställa förundersökningen av brott som gäller terrorism på det sätt som avtalats med skyddspolisen och Polisstyrelsen.

Skyddspolisen kan även inleda förundersökningen av olaga hot eller ett annat liknande brott som riktas mot en person som hör till statens ledning och som kommit till dess kännedom om gärningen uppenbart har att göra med rikets inre eller yttre säkerhet och om det är nödvändigt att omedelbart inleda förundersökningen för att skyndsamt verkställa förebyggande åtgärder. När förundersökningen fortsätter ska utredningen utan dröjsmål överföras till en annan polisenhet.

De övriga polisenheterna bistår skyddspolisen i förundersökningen på det sätt som avtalats med Polisstyrelsen. Skyddspolisen bistår och samarbetar med den enhet som verkställer förundersökningen även i förundersökningar av andra brott som är av betydelse för Finlands inre och yttre säkerhet än de ovan nämnda. Till exempel gärningar som nämns i strafflagens 11 och 14 kap. är sådana.

Arbetsgruppen som dryftade skyddspolisens administrativa ställning, resultatstyrning samt övervakning skulle även bedöma behoven att utveckla skyddspolisens verksamhet inför kommande hot mot säkerheten. Det centrala syftet var att klargöra skyddspolisens verksamhetsförutsättningar, befogenheter och övervakning med beaktande av den nationella och den internationella operativa situationen samt säkerhetstjänsternas internationella utvecklingstrender.

Enligt den aktuella arbetsgruppen bör det bildas en mekanism för att årligen ställa upp prioriteringar för skyddspolisens informationsinhämtning som fungerar så att detta sker under ledning av inrikesministeriet. Innan prioriteringarna fastställs ska de beredas och samordnas i statsrådets utrikes- och säkerhetspolitiska ministerutskott och det bör ges en rapport om dem till riksdagens berörda utskott (grundlagsutskottet, utrikesutskottet och förvaltningsutskottet).

Arbetsgruppen ansåg att man bör överväga nya befogenheter för underrättelseinhämtning för skyddspolisen för att den ska kunna svara på de ändrade verksamhetsbetingelserna. Det gäller inhämtande av uppgifter som är nödvändiga för att avvärja projekt som äventyrar rikets säkerhet av personer som är informationskällor och från datanät trots att projekten inte har uppnått graden för brott som kan förhindras, avslöjas eller utredas. När saken övervägs måste de juridiska förutsättningarna för att eventuellt utvidga befogenheterna för underrättelseinhämtning utredas mer ingående bland annat ur perspektivet för de grundläggande och mänskliga rättigheterna.

Det finns redan i nuläget bestämmelser om mottagande av information från personer som är informationskällor för att förhindra eller avslöja brott eller avvärja en fara i 5 kap. i polislagen och användning av informationskällor för att utreda brott i 10 kap. i tvångsmedelslagen. Hemligt inhämtande av information kan tryggas enligt polislagen och tvångsmedelslagen och det kan också användas i samband med användningen av informationskällor. Det måste övervägas om bestämmelserna om användandet av informationskällor och tryggandet av dem ska utsträckas till att uttryckligen också gälla avvärjandet av projekt som äventyrar rikets säkerhet.

Vid användningen av informationskällor bör information kunna inhämtas även från utlandet för att förhindra projekt som äventyrar rikets säkerhet. Innan man börjar inhämta information från utlandet bör man utöver de krav som Finlands nationella lagstiftning ställer dessutom från fall till fall beakta de internationella skyldigheter som är bindande för Finland och den nationella lagstiftningen i den stat som man avser inhämta information från. Förutsättningarna för att arbeta utomlands samt förhållandena för styrningen av och ansvaret för verksamheten bör preciseras i samband med en eventuell fortsatt beredning av nationella bestämmelser. Eftersom inhämtande av information utomlands också kan röra aspekter kring Finlands internationella relationer bör man innan man börjar inhämta sådan information förhandla åtminstone med det ministerium (den del av statsrådet) som leder skyddspolisen och med utrikesministeriet.

Arbetsgruppen konstaterade rätt entydigt att om skyddspolisens befogenheter att inhämta underrättelser utökas bör man för att trygga en rättvis rättegång överväga att begränsa skyddspolisens uppgifter och befogenheter vad gäller förundersökningar. Då ska skyddspolisen också ha prövningsrätt i fråga om hur och i vilket skede den anmäler brottsmisstankar som kommit till dess kännedom till den egentliga förundersökningsmyndigheten. Skyddspolisen ska fortfarande enligt behov få delta i förundersökningen i sin egenskap av sakkunnig myndighet.

Arbetsgruppen som bedömde skyddspolisens administrativa ställning, resultatstyrning och övervakning bedömde som enda så kallade nya befogenhet att användningen av informationskällor utsträcks till att omfatta underrättelseverksamhet som avser utländska förhållanden. Vad gäller den utvidgningen kom arbetsgruppen till slutsatsen att skyddspolisens uppgifter och befogenheter inom förundersökningarna bör begränsas. I denna proposition föreslås bestämmelser om civil underrättelseverksamhet som ska genomföras både i Finland och utomlands och om de metoder för underrättelseinhämtning som ska användas där, så det är uppenbart att det bör övervägas att skyddspolisens uppgifter och befogenheter inom förundersökningarna begränsas eller avskaffas helt.

3 Målsättning och de viktigaste förslagen

3.1 Mål

I motiveringsavsnitten till propositionens allmänna motivering och detaljmotivering har redan behandlats vissa frågor i anslutning till tryggandet av de grundläggande och mänskliga rättigheterna till den del som de har betydelse för utformningen och tolkningen av de föreslagna bestämmelserna. I detta avseende har i beredningen beaktats Europadomstolens praxis samt grundlagsutskottets ställningstaganden.

Den internationella säkerhetsmiljön förändras snabbt. Bland annat i brytningstiden som skett i verksamhetsbetingelserna med hybridpåverkan och digitalisering måste Finland ännu bättre än tidigare kunna inhämta information som baseras på fenomen och hot. Lagstiftningen behöver utvecklas för att man ska kunna handla i den förändrade verksamhetsmiljön. Med de nuvarande befogenheterna för brottsbekämpning kan man inte i ett tillräckligt effektivt skede upptäcka hot som äventyrar samhällets säkerhet eller vidta de åtgärder som krävs. Spridandet och användningen av oriktig information betonar säkerhetsmyndigheternas behov av att producera objektiv, bekräftad och analyserad information som stöd för den högsta statsledningens beslutsfattande. Därför bör den rättsliga grunden för underrättelsemyndigheternas inhämtande av information utvecklas. Det viktigaste målet med lagstiftningen som föreslås är att förbättra den nationella säkerheten. Målet är att förbättra det finländska samhällets möjligheter att skydda sig mot allvarliga hot som riktas mot den nationella säkerheten. Målet med lagstiftningen är fortfarande att stödja beslutsfattandet i statens högsta ledning och säkerställa att det grundar sig på riktig, aktuell och tillförlitlig information. Genom lagstiftningen görs det även möjligt för skyddspolisen och de andra myndigheterna inom nationell säkerhet att börja bekämpa hot i ett tidigt skede. Skyddspolisens informationsinhämtning förbättras också när allvarliga internationella hot hör till dess uppgifter så att skyddspolisen ska ha reella möjligheter att klara av sina lagstadgade uppgifter.

Arbetsgruppen för en informationsanskaffningslag har i sitt betänkande föreslagit att det bör skapas en rättslig grund i Finland för underrättelseinhämtning som avser datatrafikspaning, personbaserad underrättelseinhämtning utomlands och spaning i utländska datasystem. Dessutom är det nödvändigt att skapa en rättslig grund för befogenheter för underrättelseinhämtning i Finland av samma orsaker som för underrättelseverksamhet som avser utländska förhållanden. Trots att de allvarligaste hoten som riktas mot Finland huvudsakligen är av utländskt ursprung kan ett sådant hot genomföras även i Finland. Inhämtandet av information för att avvärja hot måste vara effektivt oberoende av hur nära hotet finns. Det torde vara självklart att ju närmare Finland ett hot är desto mer motiverat är det att inleda åtgärderna för inhämtande av underrättelser omedelbart.

De typer av underrättelseinhämtning som arbetsgruppen för en informationsanskaffningslag avser ersätter inte varandra eftersom de till karaktären delvis är olika. Avsikten med underrättelseinhämtning som avser datatrafik är framför allt att upptäcka aktivitet som allvarligt hotar den nationella säkerheten. Genom personbaserad underrättelseinhämtning och underrättelseinhämtning som avser datasystem inhämtas huvudsakligen information om identifierade hot. Befogenheterna för underrättelseinhämtning bildar således en helhet som består av flera olika metoder för underrättelseinhämtning som kompletterar varandra. Som framgår av den internationella jämförelsen har staternas underrättelsemyndigheter jämförbara befogenheter avsedda för underrättelseinhämtning som det i Finland finns bestämmelser om enbart för behov inom brottsbekämpning. Genom befogenheterna för brottsbekämpning är det inte möjligt att få all information som är nödvändig för den nationella säkerheten.

Denna regeringsproposition innehåller ett förslag till en helhet som gäller lagstiftning om civil underrättelseverksamhet. Lagförslagen är skrivna så att skyddspolisens och de andra myndigheternas befogenheter, rättigheter och skyldigheter framgår tillräckligt exakt och skarpt avgränsat av dem. I beredningen av lagförslaget har man försökt begränsa ingripanden i skyddet av de grundläggande rättigheterna så mycket som möjligt med hänsyn till de krav som verksamhetens effektivitet och resultat ställer. I beredningen har man fäst särskild uppmärksamhet vid internationella fördrag om mänskliga rättigheter som är förpliktande för Finland samt vid beslutspraxis som gäller Europeiska människorättskonventionen och i Europeiska unionens domstol.

Målen med lagstiftningen om underrättelseinhämtning som avser datatrafik

På grund av särdragen i underrättelseinhämtning som avser datatrafik föreslås det att det stiftas en egen lag om den. Den är trots det en sammanhängande del av en mer omfattande helhet av civil underrättelseverksamhet. Syftet med alla metoder för underrättelseinhämtning, även den som avser datatrafik, är att producera nödvändig information som stöd för beslutsfattandet i den högsta statsledningen. Dessutom är syftet med underrättelseinhämtning att möjliggöra utformningen av en aktuell bild av säkerhetsläget, att ha beredskap inför allvarliga hot mot den nationella säkerheten och att avvärja hoten.

Användningen av underrättelseinhämtning som avser datatrafik kräver, på samma sätt som de andra metoderna för underrättelseinhämtning, alltid faktabaserad information om att ett allvarligt hot mot den nationella säkerheten existerar och om grundläggande faktum om hotet. Information om att hotet existerar kan ha erhållits till exempel inom ramen för nationellt myndighetssamarbete eller internationellt samarbete för underrättelseinhämtning.

Utöver de övergripande målen som ställs för civil underrättelseverksamhet har underrättelseinhämtning som avser datatrafik beroende på sina särdrag en viktig funktion genom att den kompletterar övriga metoder för underrättelseinhämtning och användningen av dem. Metodernas särskilda karaktär möjliggör lokalisering av källorna till hot som riktas mot den nationella säkerheten och till att de som finns i bakgrunden för hoten kan identifieras. De observationer som görs med hjälp av underrättelseinhämtning som avser datatrafik är i många fall en nödvändig förutsättning för att andra metoder för underrättelseinhämtning som grundar sig på ett annat slag av logik för hur de riktas enligt polislagens 5 a kap. kan användas över huvud taget.

Ett särskilt mål med lagstiftningen är även att förbättra Finlands förmåga att skydda sig mot allvarliga hot mot datanäten. Förutsättningen för att förhindra eller åtminstone att begränsa de skadliga effekter som orsakas av hot mot datanäten är att de upptäcks i ett tillräckligt tidigt skede. Underrättelseinhämtning som avser datatrafik kan bedömas förbättra förmågan att i betydande utsträckning upptäcka speciellt cyberdåd som utförs med hjälp av skadliga datorprogram där statliga aktörer ligger i bakgrunden. Bland annat en färsk undersökning som beskriver nuläget i Finlands cybersäkerhet och målbild (Publikationsserie för statsrådets utrednings- och forskningsverksamhet 30/2017) och Norges så kallade Lysne II –kommittés slutbetänkande (Digital Grenseforsvar (DGF) från 2016 fäster uppmärksamhet vid den stora betydelse underrättelseinhämtning som avser datatrafik har för samhällets förmåga att skydda sig mot cyberhot. Lagstiftning om underrättelseinhämtning som avser datatrafik kompletterar på så sätt observationssystemet som grundar sig på bestämmelserna om den nuvarande lagen om tjänster inom elektronisk kommunikation speciellt vad gäller de allra allvarligaste hoten mot datanäten.

I avsnittet om internationell jämförelse behandlas lagstiftningen om underrättelseinhämtning i sex europeiska stater. För två år sedan hade endast två av jämförelsestaterna, Sverige och Tyskland, lagstiftning om underrättelseinhämtning som avser datatrafik. Efter det har också

tre av de andra staterna reglerat detta eller börjat bereda lagstiftning om det. I jämförelsestaternas handlingar för beredningen betonas kraftigt betydelsen av underrättelseinhämtningen som avser datatrafik som en av metoderna i helheten av metoder för underrättelseinhämtning.

Lagstiftning om underrättelseinhämtning som avser datatrafik kan bedömas märkbart förbättra till exempel Finlands förmåga att förhindra terrorism. Som en internationell jämförelseuppgift är det motiverat att nämna att Sveriges säkerhetspolis i januari 2015 meddelade att den under föregående ett och ett halvt år hade förhindrat två terrordåd med hjälp av underrättelseinhämtning som avser datatrafik som den fått av signalunderrättelsetjänsten. Det är exceptionellt att informera om saken, för länder som har lagstiftning om underrättelseinhämtning behandlar av sekretesskäl i allmänhet inte i offentligheten genom vilken uttrycklig metod för underrättelseinhämtning några speciella uppgifter om hot har inhämtats.

Arbetsgruppen för en informationsanskaffningslag hörde utländska experter för att klargöra vilken betydelse underrättelseinhämtning som avser datatrafik har för det statliga beslutsfattandet. De som hördes betonade denna underrättelseinhämtnings betydelse i inhämtandet av strategisk information som grund för statens högsta beslutsfattande. Enligt dem kan modernt utrikes- och säkerhetspolitiskt beslutsfattande endast grunda sig på tidsenlig underrättelseinformation till vilken datatrafikspaningen bidrar med en viktig del (s. 72 i betänkandet).

Lagen om civil underrättelseinhämtning avseende datatrafik som enligt förslaget ska stiftas grundar sig på en skrivning i det strategiska regeringsprogrammet för statsminister Juha Sipiläs regering enligt vilken regeringen föreslår att det skapas en rättsgrund för underrättelseinhämtning som avser datatrafik, och på betänkandet från arbetsgruppen för en lag om inhämtandet av information som ligger bakom skrivningen. Till den del lagförslaget avviker från arbetsgruppens ställningstaganden behandlas orsaken till och karaktären för avvikelsen nedan bland de viktigaste förslagen.

Lagen om civil underrättelseinhämtning avseende datatrafik som föreslås är skriven så att befogenheterna, rättigheterna och skyldigheterna för de aktörer som deltar i underrättelseinhämtning som avser datatrafik exakt framgår av lagen. I beredningen av lagförslaget har man försökt begränsa ingripanden i skyddet av de grundläggande rättigheterna så mycket som möjligt med hänsyn till de krav som verksamhetens effektivitet och resultat ställer. Lagen innehåller flera begränsningar som satts för användning av underrättelseinhämtning som avser datatrafik i syfte att skydda kommunikationshemligheten som inte har någon motsvarighet i jämförelsestaterna. Den mest betydande av dem gäller att man i underrättelseinhämtning som avser datatrafik inte ska få använda sökbegrepp som beskriver innehållet i ett meddelande annat än i noggrant avgränsade undantagsfall.

Omfattningen av hur underrättelseinhämtning som avser datatrafik ingriper i datakommunikationen behandlas bland annat i avsnittet om konsekvenser för informationssamhället.

3.2 Alternativ

Utvidgande av användningsområdet för befogenheterna för brottsbekämpning

I nuläget finns det ingen lagstiftning i Finland om underrättelseinhämtning och inga föreskrifter om särskilda befogenheter för skyddspolisen att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten. Skyddspolisen fullgör sin uppgift genom att använda de befogenheter som reglerar polisens verksamhet i allmänna lagar.

Det är möjligt att utvidga användningsområdet för befogenheterna för brottsbekämpning till exempel genom att reglera att verksamhet som allvarligt hotar den nationella säkerheten blir

straffbar i större utsträckning än i nuläget och att på motsvarande sätt utvidga området för brott som under särskilda villkor utgör en grund för användning av hemliga metoder för informationsinhämtning.

Om ett sådant alternativ övervägs måste man beakta att strafflagen begränsas av grundlagen och internationella förpliktelser i fråga om mänskliga rättigheter som är bindande för Finland. Begränsningarna i grundlagen beror väsentligast på de grundläggande rättigheterna. De sätter gränser för vilka gärningar som regleras som straffbara och hurdana straff eller andra påföljder som kan påföras för brott. När man beaktar de gällande befogenheterna som baserar sig på brott är bristen på befogenheter i fråga om de nuvarande utredningsmetoderna eller förhindrandet av brott därför inte i sig en grund för att reglera gärningar som straffbara. När behoven att kriminalisera diskuteras lyfts det då och då fram som skäl för kriminalisering att myndigheterna inte har befogenheter att ingripa i ett visst beteende som anses vara negativt om beteendet inte kriminaliseras. Denna aspekt har tagits upp även i samband med lagstiftningsprojekten om civil underrättelseverksamhet. Ingen gärning kriminaliseras dock för att hemliga metoder för inhämtande av information enligt polislagen ska kunna användas för att förhindra eller avslöja den. Om det på basis av de allmänna förutsättningarna för tillämpning av strafflagstiftning och kriminaliseringsprinciperna finns tillräckliga grunder för att kriminalisera en gärning ska användningen av de metoder för inhämtande av information som behövs för att förhindra och utreda en gärning prövas och bedömas särskilt. Möjligheten att i omfattande grad använda metoder för inhämtande av information enligt polislagen i stor utsträckning utgör inte heller någon betydande grund vid regleringen av straffskalan för ett brott (se t.ex. RP 18/2014 rd s. 13).

Nedan i propositionen behandlas verksamhet som är föremål för civil underrättelseverksamhet och som allvarligt hotar den nationella säkerheten. Tidigare i förslaget har det också konstaterats att det finns hot som inte kan utvecklas till brott, såsom till exempel ändrade ägarförhållanden som äventyrar Finlands försörjningsberedskap eller verksamhet där en främmande stat kartlägger strukturen i datanät för datatekniska styrsystem i nätverk för europeisk energidistribution och tekniska sårbarheter i syfte att eventuellt utnyttja informationen för att slå ut elnätet. Kriminalisering som går så långt eller är så vid är problematisk med tanke på den straffrättsliga legalitetsprincipen. På grund av kravet på att en begränsning ska vara godtagbar med hänsyn till de grundläggande rättigheterna ska det finnas ett vägande samhälleligt behov och en acceptabel grund för kriminalisering. Till exempel skyldigheten att skydda en grundläggande rättighet kan vara en godtagbar grund för kriminalisering (GrUU 23/1997 rd). Brottsrekvisitet ska dessutom anges tillräckligt exakt i lagen för att det utifrån bestämmelsens lydelse ska gå att sluta sig till om en handling eller försummelse är straffbar (se t.ex. GrUU 38/2012 rd s. 4, GrUU 68/2010 rd s. 4, GrUU 58/2010 rd, s.3, GrUU 33/2010 rd s 2–3, GrUU 12/2010 rd, s. 3, GrUU 17/2006 rd, s 3–4). De ovan relaterade förutsättningarna kan utgöra betydande utmaningar eller ett direkt hinder för att någon typ av den verksamhet som nämnts ska kriminaliseras.

Under projektet för en lag om underrättelseinhämtning har det också föreslagits att underrättelseinhämtning som avser datatrafik kan ersättas genom att utvidga tillämpningsområdet för användning av teleavlyssning och teleövervakning materiellt och områdesmässigt sett.

I denna proposition föreslås det att det materiella och områdesmässiga tillämpningsområdet för användning av teleavlyssning och teleövervakning utvidgas som grund för underrättelseinhämtning, men inte via kriminalisering. Dessutom ska enligt förslaget det territoriella tillämpningsområdet för befogenheterna för underrättelseinhämtning utvidgas till att gälla utanför Finland. Detta undanröjer dock inte behovet att reglera en egen befogenhet för underrättelseinhämtning som avser datatrafik. Teleavlyssning och teleövervakning som metoder lämpar sig inte för att upptäcka brott eller hot eller för identifiering av personerna i bakgrunden för det

oberoende av hur det materiella eller territoriella användningsområdet har definierats. Som metoder lämpar de sig inte heller för att upptäcka hot mot datanäten eller informationsinhämtning om dem.

Det är motiverat att utvidga användningsområdet för teleavlyssning och teleövervakning i stället för reglering om underrättelseinhämtning som avser datatrafik speciellt av den orsaken att det först nämnda alternativet till åtskillnad från det andra inte grundar sig på filtrering av datakommunikation och därför inte gör det möjligt för myndigheter att få tillträde till konfidentiell kommunikation hos personer som inte har någon koppling till allvarliga brott. Trots att uppmärksamheten för de finländska myndigheternas del stämmer medför inte det att konfidentiell kommunikation hos finländska personer i utomstående ställning inte redan i nuläget är föremål för underrättelseinhämtning. Det finns numera datatrafikförbindelser via undervattens- och jordkablar från Finland till Sverige, Tyskland, Estland och Ryssland. Det framgår av den internationella jämförelsen i detta betänkande och av beskrivningen av internationell rättspraxis att av dem åtminstone Sverige, Tyskland och Ryssland bedriver underrättelseinhämtning riktad mot datakommunikationsförbindelser, alltså även från Finland, som överskrider de egna statsgränserna. Härav följer att de datatrafikförbindelser som går från Finland och den finländska konfidentiella kommunikationen redan nu heltäckande finns med som föremål för underrättelseinhämtning som grundar sig på filtrering av datatrafik som främmande makter bedriver. Denna underrättelseinhämtning som omfattar finländarnas konfidentiella kommunikation bedrivs inte för att skydda Finlands nationella säkerhet utan i de främmande staternas egna intressen och syften.

Förutom det ovan sagda är det inte möjligt att använda befogenheter för brottsbekämpning utanför Finlands gränser beroende på det territoriella tillämpningsområdet för användningen av dem.

På de ovan nämnda grunderna är det inte motiverat att användningsområdet för de nuvarande befogenheterna för brottsbekämpning utvidgas.

Förslag från arbetsgruppen för en informationsanskaffningslag

Arbetsgruppen för en informationsanskaffningslag föreslog i sitt betänkande att det för de militära och civila myndigheter som ansvarar för den nationella säkerheten regleras om befogenheter för personbaserad underrättelseinhämtning utomlands, spaning i utländska datasystem och underrättelseinhämtning som avser gränsöverskridande datakommunikation. Skyddspolisen var den civila myndighet som enligt arbetsgruppen ansvarar för den nationella säkerheten.

Med personbaserad underrättelseinhämtning utomlands avsågs i betänkandet av arbetsgruppen för en informationsanskaffningslag underrättelseinhämtning utomlands som baserar sig på personligt umgänge med eller personlig observation av en person eller ett annat objekt. Med spaning i utländska datasystem avsågs å sin sida inhämtning av information som behandlas i utländska datasystem med datatekniska metoder. Med datatrafikspaning avsåg underrättelseinhämtning som riktas mot datatrafik i datatrafikkablar som överskrider Finlands gränser.

I förslaget från arbetsgruppen för en informationsanskaffningslag om spaning i utländska datasystem och personbaserad underrättelseinhämtning utomlands var det frågan om verksamhet som sker utomlands (underrättelseinhämtning som avser utländska förhållanden).

Avsikten både vad gäller datatrafikspaning och spaning i utländska datasystem var enligt arbetsgruppens förslag att inhämta nödvändig information via underrättelseinhämtning om allvarliga internationella hot mot den nationella säkerheten. Genom verksamheten stöds statens högsta lednings beslutsfattande och säkerställs att det grundar sig på riktig, aktuell och tillför-

litlig information. Genom verksamheten görs det även möjligt för de behöriga myndigheterna att inleda bekämpningen av hot.

Gränssnittet mellan underrättelseinhämtning och bekämpningsåtgärder organiseras separat. Med anledning av den information som underrättelseinhämtningen producerar kan den behöriga myndigheten börja vidta de åtgärder som behövs för att avvärja ett hot.

Underrättelseinhämtningen ska övervakas såväl juridiskt som parlamentariskt. Det är relevant att ordna övervakningen av olika metoder för underrättelseinhämtning så enhetligt som möjligt.

Arbetsgruppen för en informationsanskaffningslag föreslog att befogenheterna inom civil underrättelseverksamhet bereds vid inrikesministeriet och befogenheterna inom militär underrättelseverksamhet vid försvarsministeriet. Eftersom underrättelseinhämtning som avser datatrafik behövs inom båda förvaltningsområdena bör det övervägas om en separat lag bör stiftas om underrättelseinhämtning som avser datatrafik.

Arbetsgruppen för en informationsanskaffningslag tog dock inte ställning för var det ska regleras om övervakningsmekanismer om befogenheter, beslutsfattande och underrättelseinhämtning som ligger på inrikesministeriets eller försvarsministeriets föredragningsansvar utan lämnade avgörandet om lagstiftningen öppet till dessa delar.

Förslag från lagarbetsgruppen för civil underrättelseinhämtning

Denna regeringsproposition grundar sig på huvudsakligen på betänkandet från lagarbetsgruppen för civil underrättelseinhämtning.

Lagarbetsgruppen för civil underrättelseinhämtning omfattade i sitt arbete de centrala lösningarna från arbetsgruppen för en informationsanskaffningslag. Medan arbetet framskred tog lagarbetsgruppen för civil underrättelseinhämtning emellertid upp behoven av befogenheter som ett mer övergripande föremål för granskning än arbetsgruppen för en informationsanskaffningslag. Lagarbetsgruppen för civil underrättelseinhämtning ansåg det motiverat att användningen av befogenheterna för underrättelseverksamhet som avser utländska förhållanden, det vill säga personbaserad underrättelseinhämtning och underrättelseinformation som avser datasystem, möjliggörs även i Finland. Enligt arbetsgruppens uppfattning bör användningen av befogenheterna möjliggöra en tillräckligt effektiv och heltäckande informationsinhämtning om de allvarligaste hoten mot den nationella säkerheten oberoende av hotets geografiska läge. Trots att de allvarligaste hoten mot den nationella säkerheten ofta gäller händelser utanför Finland kan följderna av ett hot realiseras i Finland. Befogenheter för underrättelseinhämtning kan anses nödvändigare ju närmare Finland hotet är beläget. Befogenheter för underrättelseinhämtning kan anses nödvändiga i en situation där ett hot har kommit innanför Finlands gränser. En arbetsgrupp som berett lagstiftning för militär underrättelseverksamhet har kommit till motsvarande lösning.

Lagarbetsgruppen för civil underrättelseinhämtning hade fyra olika alternativ till ramverk för lagstiftning om civil underrättelseverksamhet. Enligt det första alternativet skulle alla bestämmelser om civil underrättelseverksamhet ha inkluderats i en lag om civil underrättelseverksamhet. I det andra alternativet skulle personbaserad underrättelseinhämtning och underrättelseinhämtning som avser datasystem ha ingått i en lag om civil underrättelseverksamhet och underrättelseinhämtning avseende datatrafik i civil underrättelseverksamhet i en egen lag. Enligt ett tredje alternativ skulle alla bestämmelser om civil underrättelseverksamhet inkluderas i polislagens nya 5 a kap. Enligt det fjärde alternativet, som arbetsgruppen valde, ska personbaserad underrättelseinhämtning och underrättelseinhämtning som avser datasystem regle-

ras i polislagens nya 5 a kap. och underrättelseinhämtning som avser datatrafik i en egen lag om civil underrättelseinhämtning avseende datatrafik.

Det sistnämnda alternativet ansågs vara det mest ändamålsenliga som ram för lagstiftning om civil underrättelseverksamhet. För det talar bland annat det faktum att skyddspolisen är en polisenhet och bestämmelserna som gäller polisen tillämpas på dess verksamhet. I polislagens 1 kap. anges polisens uppgift och de principer som styr polisens verksamhet såsom principen att respektera de grundläggande och mänskliga rättigheterna, proportionalitetsprincipen, principen om minsta olägenhet och principen om ändamålsbundenhet samt om åtgärdseftergift och åtgärdsfördröjning.

I 5 kap. i polislagen anges de befogenheter som skyddspolisen använder för informationsinhämtning i nuläget, hemliga metoder för inhämtande av information. Personbaserad underrättelseinhämtning och underrättelseinhämtning som avser datasystem kan indelas i befogenheter som regleras i det aktuella kapitlet i polislagen. Personbaserad underrättelseinhämtning indelas i teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk observation (med undantag av teknisk observation av utrustning och delvis teknisk avlyssning), inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp och användning av informationskällor. Teknisk observation av utrustning omfattar underrättelseinhämtning som avser datasystem och teknisk avlyssning till vissa delar. Därför behöver det till stor del inte regleras om helt nya befogenheter. Däremot är det nödvändigt att reglera grunderna för användningen av befogenheterna på ett sätt som lämpar sig för underrättelseverksamhet.

Saken kan åskådliggöras genom de gällande befogenheterna. Hemliga metoder för inhämtande av information enligt polislagens 5 kap. får användas för förhindrande, avslöjande eller avvärjande av risk för brott, medan hemliga metoder enligt tvångsmedelslagens 10 kap. får användas för att utreda ett brott. Det föreslås att metoderna för underrättelseinhämtning i polislagens nya 5 a kap. ska användas för att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten. Med hänsyn till det ovan nämnda är det motiverat att metoderna i 5 a kap. till tillvägagångssätten baseras på de hemliga metoderna för inhämtande av information enligt 5 kap. i polislagen.

Underrättelseinhämtning som avser datatrafik och som överskrider Finlands gränser regleras enligt förslaget i lagen om civil underrättelseinhämtning avseende datatrafik. För underrättelseinhämtning som avser datatrafik och befogenheterna i polislagens 5 a kap. används benämningen metoder för underrättelseinhämtning.

3.3 De viktigaste förslagen

Polislagen

I det nya 5 a kap. som föreslås i polislagen ska metoderna för underrättelseinhämtning inom civil underrättelseverksamhet regleras. Definitionen av civil underrättelseverksamhet ska finnas i 1 § i kapitlet. Enligt paragrafen avses med civil underrättelseinhämtning sådant inhämtande av information och utnyttjande av informationen som skyddspolisen utför för att skydda den nationella säkerheten till stöd för beslutsfattandet i den högsta statsledningen samt för övriga myndigheters lagstadgade uppgifter som har samband med den nationella säkerheten. Det gäller en ny uppgift för skyddspolisen som gör det nödvändigt att också ändra bestämmelsen om polisens uppgifter i 1 kap. 1 § 1 mom. samt bestämmelsen om skyddspolisens uppgifter i 10 § i polisförvaltningslagen.

Bestämmelserna som fastställer skyddspolisens uppgift utgör dock inte i sig någon grund för en allmän befogenhet för skyddspolisen att vidta nödvändiga åtgärder för att skydda den nationella säkerheten. Definitionerna av uppgifterna är emellertid en utgångspunkt vid bedömningen om åtgärder som skyddspolisen ska tillåtas använda i civil underrättelseverksamhet och utgör grunden för tolkningen av de nya befogenheterna. Om skyddspolisens befogenheter används i ett syfte som avviker från definitionen av skyddspolisens uppgifter kan det vara frågan om rättsstridigt missbruk av prövningsrätt. Principen om ändamålsbundenhet anges uttryckligen i 1 kap. 5 § i lagen.

Polislagens nya 5 a kap. föreslås få bestämmelser om andra metoder för underrättelseinhämtning i civil underrättelseverksamhet (2 §) än underrättelseinhämtning som avser datatrafik som får en egen lag om civil underrättelseinhämtning avseende datatrafik. Metoderna för underrättelseinhämtning i det nya 5 a kap. grundar sig till tillvägagångssätten på de hemliga metoderna för inhämtande av information i polislagens 5 kap. Förutsättningarna för användning av dem regleras så som det föreslås mer ingående nedan. Det föreslås bestämmelser om helt nya befogenheter om platsspecifik underrättelseinhämtning, kopiering, kvarhållande av en försändelse för kopiering och erhållande av uppgifter av en privat sammanslutning (2 § 2 mom.) samt underrättelseinhämtning som avser datatrafik (2 § 3 mom.).

I 3 § finns det enligt förslaget bestämmelser om objekten för civil underrättelseverksamhet som är: 1) terrorism, 2) utländsk underrättelseverksamhet, 3) planering, tillverkning, spridning och användning av massförstörelsevapen, 4) planering, spridning och användning av sådana produkter med dubbel användning som avses i 2 § i lagen om kontroll av export av produkter med dubbel användning (562/1992), 5) verksamhet som hotar den demokratiska samhällsordningen, 6) verksamhet som hotar ett stort antal människors liv eller hälsa eller samhällets vitala funktioner, 7) en främmande stats planer eller verksamhet som kan orsaka skada för Finlands internationella relationer, ekonomiska intressen eller andra viktiga intressen, 8) en kris som hotar internationell fred och säkerhet, 10) verksamhet som hotar internationella krishanteringsinsatser, och 11) internationell organiserad brottslighet som hotar samhällsordningen.

De ovan nämnda objekten för civil underrättelseverksamhet eller de så kallade grundläggande hoten anses sortera under begreppet nationell säkerhet huvudsakligen på det sätt som Europeiska domstolen för de mänskliga rättigheterna har tolkat begreppet. Förteckningen över objekt ska vara uttömmande och sätter gränser för skyddspolisens användning av sina befogenheter.

Förutsättningarna för användning av en metod för underrättelseinhämtning regleras i 4 §. I paragrafens 1 mom. regleras kravet på resultat som en grund som gäller förutsättningarna för alla metoder för underrättelseinhämtning. Den allmänna förutsättningen för att en metod för underrättelseinhämtning ska få användas är att man genom den med fog kan antas få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten. För varje användning av en metod för underrättelseinhämtning bör man kunna påvisa att grunden för ett hot som nämns i förteckningen över objekt existerar, och att grunden även utgör ett allvarligt hot mot den nationella säkerheten. Därför kan vilket objekt för den civila underrättelseverksamheten som helst i sig inte utgöra ett allvarligt hot för den nationella säkerheten.

Med verksamhet som allvarligt hotar den nationella säkerheten avses i sista hand ett yttre hot om våld som omedelbart eller indirekt riktas mot den kollektiva säkerheten hos människorna som omfattas av statens jurisdiktion. Våldsdåd som riktas till exempel mot enskilda personer kan emellertid vara verksamhet som avses i bestämmelsen om de till sin omfattning eller betydelse är betydande med tanke på samhällets kollektiva säkerhetsintressen och på så sätt kan utgöra ett allvarligt hot mot dem. Med uttrycket ”hot” avses situationer där den nationella säkerheten inte omedelbart håller på att äventyras. Inhämtandet av information kan då också

gälla verksamhet som om den fortsätter kan äventyra den nationella säkerheten. Ett hot som allvarligt hotar den nationella säkerheten är typiskt sett en allmänfarlig verksamhet och aktivitet som har samband med den och som hotar en stor och oförutsedd, slumpmässigt bestämd grupp människors liv eller hälsa. Med hänsyn till den nationella säkerheten är sådana basfunktioner i samhället centrala som om de störs eller lamslås indirekt kan leda till att människors liv eller hälsa äventyras allvarligt. Med verksamhet som allvarligt hotar den nationella säkerheten avses även verksamhet som hotar den demokratiska stats- och samhällsordningen, samhällets basfunktioner, ett stort antal människors liv eller hälsa eller internationell fred och säkerhet.

Särskilda förutsättningar för användningen av vissa metoder för underrättelseinhämtning regleras enligt förslaget i 4 § 2 mom. De metoderna för underrättelseinhämtning får användas endast om man med fog kan anta att de har en synnerligen viktig betydelse när det gäller att få uppgifter om verksamhet som avses i 1 mom. Användning av täckoperationer och bevisprovokation genom köp förutsätter dessutom att användningen av metoden är nödvändig. En förutsättning för täckoperationer är dessutom att inhämtandet av information måste anses vara behövligt på grund av att verksamheten är planmässig, organiserad eller yrkesmässig eller det kan antas att den fortsätter eller upprepas. I 3 mom. regleras en lägre tröskel för användningen av en metod för underrättelseinhämtning i de fall den riktas mot en statlig myndighet eller en jämförbar aktör. I paragrafens 4 mom. finns en begränsning som gäller användningen av alla metoder för underrättelseinhämtning enligt vilken de inte får riktas mot utrymmen som används för stadigvarande boende. Endast täckoperationer och bevisprovokation genom köp är undantag och får användas i en bostad om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden. Detta har att göra med risken för att de aktuella metoderna för underrättelseinhämtning avslöjas. I 5 mom. finns ett krav enligt vilket användning av en metod för underrättelseinhämtning ska avslutas före utgången av den tid som anges i beslutet om syftet med användningen har nåtts eller om det inte längre finns förutsättningar för att använda den. Detta har en klar betydelse beroende på den maximala tiden på sex månader för ett tillstånd om användningen av metoder för underrättelseinhämtning och speciellt på grund av principen om minsta olägenhet.

I kapitlets 5 § regleras enligt förslaget fortsatt inhämtande av information för att förhindra och avslöja brott under giltighetstiden för ett tillstånd eller beslut med stöd av 5 a kap. Det gäller skyddspolisens så kallade inre brandmur. Det föreslås att skyddspolisens uppgift även i fortsättningen ska vara att förhindra och avslöja brott som avses i 5 kap. 3 § i polislagen. Således skulle skyddspolisen enligt den bestämmelse om brandmur som föreslås i 44 § i fråga om brott enligt 5 kap. 3 § göra en anmälan till sig själv om det under användningen av en metod för underrättelseinhämtning framgår att det planeras ett brott med avsikten landsförräderi, spionerі eller i terroristiskt syfte och att brottet dessutom kan förhindras.

Förutsättningarna för användning av grunderna för metoderna för underrättelseinhämtning i 5 kap. regleras i det nya 5 a kap. så som ovan relaterats, och därför behöver det inte finnas definitioner av metoder för informationsinhämtning i 5 a kap., eftersom hemliga metoder för informationsinhämtning och metoder för underrättelseinhämtning till sina tillvägagångssätt är samma metoder. Endast de nya metoderna för underrättelseinhämtning, platsspecifik underrättelseinhämtning och kopiering, definieras separat i 5 a kap. Därför ska 5 a kap. i fråga om de flesta metoderna för underrättelseinhämtning endast gälla beslutsfattandet. Till exempel regleras beslutsfattandet om teleavlyssning och andra motsvarande metoder för informationsinhämtning i kapitlets 6 §. I paragrafens 1 mom. konstateras det att beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Enligt 2 mom. kan tillstånd för teleavlyssning eller inhämtande av information i stället för teleavlyssning ges för högst sex månader åt gången. När objektet för en åtgärd är en person kan tillståndet ges för högst tre månader åt

gången. I paragrafens 3 mom. regleras det som ska nämnas i ett yrkande och i ett beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning. De är: 1) den verksamhet som avses i 3 §, 2) den person, teleadress eller teleterminalutrustning som åtgärden riktas mot, 3) de fakta som förutsättningarna för och inriktningen av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning grundar sig på, 4) giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning, 5) den polisman som hör till befälet vid skyddspolisen som leder och övervakar utförandet av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning, och 6) eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.

För det första fastställs en tid på sex månader för tillstånd för teleavlyssning och för inhämtande av information i stället för teleavlyssning, vilket inte automatiskt innebär att tillstånd alltid kan sökas för sex månader eller att det bör beviljas för tiden sex månader. Prövningen enligt proportionalitetsprincipen och principen om minsta olägenhet kräver att uttrycket ”för högst sex månader åt gången” finns i bestämmelsen.

För det andra kan ett tillstånd för teleavlyssning gälla en person (2 punkten) i stället för en teleadress eller en teleterminalutrustning. När ett tillstånd för teleavlyssning gäller en person omfattar det de teleadresser eller den teleterminalutrustning som den personen innehar eller annars antas använda. Tillståndet för teleavlyssning gäller då inte en specifik teleadress eller teleterminalutrustning. När teleavlyssning gäller en person kan tiden för tillståndet vara endast tre månader.

Kravet på och beslutet om teleavlyssning ska innehålla de fakta som förutsättningarna för och inriktningen av teleavlyssningen eller inhämtningen av information i stället för teleavlyssning grundar sig på (3 punkten). Att faktum läggs fram för domstolen förpliktar underrättelsemyndigheten att lägga fram och motivera de faktum på grund av vilka domstolen kan dra egna slutsatser om huruvida förutsättningarna för användningen av en metod för underrättelseinhämtning uppfylls. Vad gäller förutsättningar är det för det första frågan om de allmänna förutsättningarna för användning av en metod för underrättelseinhämtning som regleras i 5 a kap. 4 §. Dessutom bör det i kravet och beslutet läggas fram tillräckliga faktum om vilken verksamhet av de objekt för civil underrättelseverksamhet som avses i 3 § som det är fråga om. I fråga om innehållet som ska ingå i kravet och beslutet för de andra punkternas del motsvarar bestämmelserna huvudsakligen 5 kap.

Beslut om teleövervakning och samtyckesbaserad teleövervakning regleras i 5 a kap. 7 § och beslut om inhämtande av basstationsuppgifter i 7 §.

Beslut om systematisk observation regleras i kapitlets 9 §. Systematisk observation kan även gälla en grupp av personer medan endast en enskild person kan utgöra objekt när systematisk observation används på grund av brott som hemlig metod för inhämtande av information eller som hemligt tvångsmedel. I civil underrättelseverksamhet kan det uppstå ett behov av att följa aktiviteten hos en viss grupp av personer. Då kan behovet av informationsinhämtning gälla gruppens organisation, personer som hör till gruppen eller gruppens aktivitet på ett visst område.

Också förtäckt inhämtande av information (10 §) kan riktas mot en person eller en grupp av personer. Såsom för de andra metoderna för underrättelseinhämtning bör man även i ett beslut om förtäckt inhämtande av information nämna de övriga faktumen i bakgrunden för informationsinhämtningen på vilkas grund en utomstående iakttagare ska ha möjlighet att dra egna slutsatser om huruvida det finns förutsättningar för användning av metoden. För beslut om förtäckt inhämtande av information ska det finnas ett undantag från att utarbeta beslutet skrift-

ligt i brådskande fall. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter att åtgärden har vidtagits.

Teknisk observation delas på samma sätt som i 5 kap. in i teknisk avlyssning, optisk observation, teknisk spårning (även teknisk spårning av person) och teknisk observation av utrustning (11–14 §). För teknisk avlyssning och för optisk observation regleras ett så kallat förfarande om brådskande beslut. Också inhämtandet av identifieringsuppgifter för teleadresser och teleterminalutrustning regleras i 5 a kap (15 §). Utrustningen som används bör vara kontrollerad av Kommunikationsverket på samma sätt som i 5 kap. Det krävs dock inte att utrustning som ska användas för att inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning ska kunna användas endast för detta ändamål. Ett sådant krav skulle göra teleavlyssning och teleövervakning mycket svåra. Genom att den tekniska utrustningens loggdata sparas kan underrättelseombudsmannen och inrikesförvaltningen övervaka användningen av den tekniska utrustningen.

I paragrafen om installation och avinstallation av anordningar, metoder eller programvara (16 §) bestäms det på avvikande sätt i förhållande till 5 kap. att (i stället för en polisman) en tjänsteman som är anställd vid skyddspolisen har rätt att fästa och avinstallera en anordning, metod eller programvara, eftersom en polisman inte nödvändigtvis i alla situationer har det tekniska kunnande som krävs för åtgärderna.

Täckoperationer och bevisprovokation genom köp regleras i 17–22 §. Kapitlet ska dock inte ha bestämmelser om deltagande i en organiserad kriminell sammanslutnings verksamhet och i kontrollerade leveranser. I 23 § regleras säkerheten för en polisman vid förtäckt inhämtande av information, vid en täckoperation, vid bevisprovokation genom köp och vid användning av informationskällor. Utöver en polisman som ska genomföra förtäckt inhämtande av information, en täckoperation eller bevisprovokation genom köp kan även en polisman som förbereder eller genomför användning av informationskällor förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att polismannens säkerhet ska kunna tryggas.

Avsikten är att ta med bestämmelser även om beslut om styrd användning av informationskällor i det nya 5 a kap. (24 §). Tryggande av informationskällor är ny befogenhet i anslutning till detta (25 §). Vid tryggande av informationskällor gäller det ett föregripande och mer intensivt skydd av en informationskälla.

I 26 § definieras platsspecifik underrättelseinhämtning. Med platsspecifik underrättelseinhämtning avses att söka efter ett föremål, egendom, dokument, information eller en omständighet i ett utrymme som inte används för stadigvarande boende eller i ett utrymme där man kan anta att det kommer att hamna information som blir objekt för underrättelseinhämtning och som man enligt 17 kap. 11, 13, 14, 16, 20, 21 § eller 22 § 2 mom. i rättegångsbalken är skyldig eller har rätt att vägra vittna om. Beslut om platsspecifik underrättelseinhämtning ska regleras i 27 §. Beslutsfattandet delas beroende på om den platsspecifika underrättelseinhämtningen riktas mot en hemfridsskyddad plats eller en plats som man inte har allmänt tillträde till eller om det allmänna tillträdet till den har begränsats eller förhindrats under den tidpunkt då den platsspecifika underrättelseinhämtningen genomförs eller inte. I det förstnämnda fallet beslutar domstolen om platsspecifik underrättelseinhämtning på yrkande av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning. I det senare fallet beslutar chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning om platsspecifik underrättelseinhämtning. I fråga om underrättande jämställs platsspecifik underrättelseinhämtning med systematisk observation, förtäckt inhämtande av information, täckoperat-

ioner, bevisprovokation genom köp och styrd användning av informationskällor om vilka man inte är skyldig att underrätta objektet för inhämtandet av information om förundersökning inte har inletts i ärendet.

I kapitlets 28 § regleras kopiering som på samma sätt som platsspecifik underrättelseinhämtning är en metod för underrättelseinhämtning. Enligt paragrafen har skyddspolisen vid civil underrättelseinhämtning rätt att kopiera en handling eller ett föremål för att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten.

Om kopieringsförbud (29 §) samt kopieringsförbud som gäller teleavlyssning, teleövervakning och basstationsuppgifter (30 §) ska det huvudsakligen regleras på samma sätt som i 7 mom. i paragrafen om beslutande om platsspecifik underrättelseinhämtning.

I kapitlets 31 § och 32 § regleras kopiering av försändelser och kvarhållande av försändelser för kopiering. Till förfarandet sett är det frågan om motsvarande metoder som anges i 7 kap. i tvångsmedelslagen. Vad gäller grunderna för användning och ändamål är det i detta sammanhang frågan om metoder för underrättelseinhämtning och därför hemlig informationsinhämtning. En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om kopiering (33 § 1 mom). En polisman vid skyddspolisen ska ha rätt att fatta ett brådskande beslut om kopiering, men beslutet ska ges en polisman som avses i 1 mom. för avgörande genast när det är möjligt (33 § 1 mom.). En kopia ska genast förstöras om det visar sig att man har kopierat material som omfattas av kopieringsförbud eller om informationen inte behövs för att skydda den nationella säkerheten (34 §).

I polislagens 5 a kap. 35 § regleras enligt förslaget förfarandet i domstol i behandlingen av ärenden om tillstånd för en metod för underrättelseinhämtning.

Skyddande av civil underrättelseinhämtning regleras i 5 a kap. 36 §. Skyddandet täcker hela den civila underrättelseverksamheten men en informationskälla eller en utomstående kan inte ges en ny identitet. Skydd får inte heller i övrigt ges på mycket lätta grunder på grund av olika problem och orsaker som gäller rättsskyddet och som har samband med saken. Därför ska det skydd som genomförs vara nödvändigt. Beslut om skyddande regleras i 37 §.

Vid användningen av en metod för underrättelseinhämtning kan man råka ut för en situation där utomstående assistans behövs eller rentav är nödvändig. Därför föreskrivs det om yppandeförbud i 38 §. Ett beslut om yppandeförbud är belagt med besvärsförbud och ändring i det kan inte sökas genom besvär. Den som fått ett förbud får dock anföra klagan utan tidsfrist. Klagan ska behandlas skyndsamt. Ett beslut om yppandeförbud bör alltid anmälas till underrättelseombudsmannen.

I 39 § regleras beslut om användning av metoder för underrättelseinhämtning på annat håll än i Finland. Vad gäller innehållet i beslutet, framställan och planen följs bestämmelserna i paragraferna om beslut om metoder för underrättelseinhämtning. För underrättelseverksamhet som avser utländska förhållanden bör man därför skriva in samma saker i ett beslut om en metod om underrättelseinhämtning som för underrättelseinhämtning i Finland. En del av bestämmelserna i 5 a kap. kan tillämpas på underrättelseverksamhet som avser utländska förhållanden. Det gäller bestämmelserna i 4 § 4 mom., 16 § 3 mom., 41, 44, 46 och 47 §.

Teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation får inte riktas mot sådan kommunikation som parterna i kommunikationen inte får vittna om med stöd av 17 kap. 13, 14, 16, 20 § eller 22 § 2 mom. i rättegångsbalken. Uppgifter som omfattas av advokathemlighet, tystnadsplikt för yrkesutbildade personer inom

hälso- och sjukvården, präster bikthemlighet och journalisters källskydd åtnjuter med stöd av bestämmelsen skydd från underrättelseinhämtning som avser datatrafik. Om det under tiden för den aktuella metoden för underrättelseinhämtning eller vid något annat tillfälle framkommer att det är fråga om ett meddelande som inte får avlyssnas eller observeras, ska åtgärden avbrytas och de upptagningar som fåtts genom åtgärden och anteckningarna om de uppgifter som fåtts genom den genast utplånas (2 mom.). Förbuden mot avlyssning och observation gäller dock inte sådana fall där en i 1 mom. avsedd person deltar i verksamhet som är objekt för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten och det också för hans eller hennes del har fattats beslut om teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation (3 mom.).

Bestämmelser om granskning av upptagningar och handlingar samt om undersökning av upptagningar finns i 42 och 43 §.

I kapitlets 44 § regleras det om en så kallad brandmur. Det gäller ett undantag från bundenheten till ett användningsändamål för information som fåtts genom metoder för underrättelseinhämtning. Regleringen om saken har utarbetats så att man på ett balanserat sätt beaktar å ena sidan användningsändamål som avviker från brottsbekämpning i underrättelseinhämtningen och å andra sidan utredningen av allvarliga brott och i synnerhet förhindrandet av sådana brott som har samband med ett betydande samhälleligt intresse. Anmälningen av lindriga brott som framkommit vid underrättelseinhämtning till brottsbekämpningen får inte vara automatisk på så sätt att underrättelseinhämtningen de facto blir en metod för att förhindra och utreda sådana brott. Å andra sidan ska också relativt lindriga brott kunna anmälas till brottsbekämpningsmyndigheterna om detta sett från fall till fall är nödvändigt för att skydda den nationella säkerheten som är syftet med underrättelseinhämtningen. Utredningen och speciellt förhindrandet av de allra allvarligaste brotten ligger å sin sida i samhällets helhetsintresse och därför finns det skäl för att i vid omfattning tillåta anmälan av dem till brottsbekämpningen. Anmälandet motiveras även av rättvisan och av att offrets perspektiv beaktas i ett allvarligt brott.

Under vissa villkor som finns i 44 § får information som erhållits genom en metod för underrättelseinhämtning utlämnas till en förundersökningsmyndighet eller en annan behörig myndighet. Information som fåtts genom underrättelseinhämtning som avser datatrafik får utan begränsning utlämnas som en utredning som stöder det att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada.

Under vissa villkor som finns i 44 § får information som erhållits genom en metod för underrättelseinhämtning utlämnas till en förundersökningsmyndighet eller en annan behörig myndighet. Information som fåtts genom användning av en metod för underrättelseinhämtning får alltid utlämnas som en utredning som stöder det att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada.

Information som fåtts genom en metod för underrättelseinhämtning ska utplånas utan dröjsmål efter att det framgått att den inte behövs för att skydda den nationella säkerheten (45 § 1 mom.). Det gäller bundenheten till ett användningsändamål för information som fåtts genom metoder för underrättelseinhämtning. Information ska dock kunna bevaras och registreras i ett register som avses i lagen om behandling av personuppgifter i polisens verksamhet om detta är nödvändigt i fall som avses i bestämmelsen om brandmuren (45 § 2 mom.).

I 46 § regleras utplåning av information som fåtts i en brådskande situation. Om en polisman som hör till befälet vid skyddspolisen i en brådskande situation enligt 7 § 1 mom., 8 § 1 mom., 11 § 1 mom., 12 § 1 mom., 13 § 1 mom., 14 § 1 mom. eller 27 § 2 mom. har beslutat att in-

hämtande av teleövervakning, basstationsuppgifter, teknisk avlyssning, optisk observation, teknisk spårning av en person, teknisk observation av utrustning eller platsspecifik underrättelseinhämtning ska inledas men domstolen anser att det inte har funnits förutsättningar för åtgärden, ska användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. I paragrafen regleras även undantag från skyldigheten att utplåna. Information som fåtts genom ett brådskande beslut får dock användas på samma villkor som i fall som avses i 44 § 1 mom. eller 2 mom. om man kan anta att ett brott har begåtts för vilket den strängaste bestraffningen är fängelse i minst sex år eller om det visar sig att det planeras ett brott för vilket den strängaste bestraffningen är fängelse i minst sex år och brottet ännu kan förhindras. I 46 § 2 mom. föreskrivs det separat om brådskande beslut om kopiering enligt vilket uppgifter får användas på motsvarande villkor som enligt 1 mom.

Underrättelse om användning av en metod för underrättelseinhämtning regleras i 47 §. Bestämmelserna i polislagens 5 kap. 58 § har använts som underlag för förslaget. Också 5 kap. 58 § 1 mom. ses över i detta sammanhang.

Efter att användningen av en metod för underrättelseinhämtning upphört ska det utan ogrundat dröjsmål upprättas ett protokoll (48 §). Mer ingående bestämmelser om vad som ska ingå i protokollet meddelas genom förordning av statsrådet. Begränsning av partsoffentlighet i vissa fall regleras i 48 §.

I 50 § regleras skyddspolisens rätt att få information av privata sammanslutningar. Bestämmelserna motsvarar till innebörden 4 kap. 3 §, men är till användningsområdet och grunderna mer noggranna och skarpt avgränsade.

I 51 och 52 § regleras teleföretags skyldighet att biträda samt tillträde till vissa utrymmen och teleföretags rätt till ersättningar på samma sätt som i 5 kap.

I 53 § regleras användningen av uppgifter som avses i 157 § 1 mom. i lagen om tjänster inom elektronisk kommunikation för att skydda den nationella säkerheten. Enligt paragrafen som föreslås kan uppgifterna användas även för att få information om verksamhet som allvarligt hotar den nationella säkerhet och som är objekt för civil underrättelseverksamhet (3 §). Det är alltså inte fråga om att bevara nya uppgifter utan om att utnyttja redan existerande uppgifter, utom för utredning av brott och för att föra dem till åtalsprövning, också för att skydda den nationella säkerheten. Mängden registrerade uppgifter ökar inte.

I slutet av 5 a kap. finns egna bestämmelser om samarbete med militärunderrättelsemyndigheten och andra myndigheter (54 §), samarbete med andra myndigheter och sammanslutningar (55 §) och samordning av hemlig informationsinhämtning (56 §).

Det finns också en separat bestämmelse om skyddspolisens internationella samarbete (57 §). Skyddspolisen kan samarbeta och genomföra informationsinhämtning i samarbete med utländsk säkerhets- och underrättelsetjänst för att skydda den nationella säkerheten utomlands och i Finland. Chefen för skyddspolisen beslutar om deltagande i internationellt samarbete och om användningen av metoder för underrättelseinhämtning i samarbete.

I 58 § föreskrivs det om samordning av den civila och den militära underrättelseverksamheten mellan republikens president, statsrådets kansli, utrikesministeriet, försvarsministeriet och inrikesministeriet och vid behov andra ministerier och myndigheter. Om det bedöms att civil underrättelseverksamhet har utrikes- och säkerhetspolitiska konsekvenser ska ärendet i förberedande syfte behandlas mellan de nämnda myndigheterna.

Bestämmelserna om övervakningen av den civila underrättelseverksamheten indelas i inrikesförvaltningens övervakning av den civila underrättelseverksamheten (59 §), extern övervakning av den civila underrättelseverksamheten (60 §) och anmälningar till underrättelseombudsmannen (61 §), vilket möjliggör övervakning av underrättelseombudsmannen i realtid i och med anmälningar som görs till skyddspolisens ombudsman. Skyddspolisen ska ge underrättelseombudsmannen information om beslut av domstol med stöd av 5 a kap. och om tillstånd så snart som möjligt efter domstolens beslut (1 mom.). Skyddspolisen ska också så snart som möjligt meddela underrättelseombudsmannen om beslut som gäller 1) annat än en metod för underrättelseinhämtning som avses i 1 mom., 2) skyddande av civil underrättelseverksamhet 3) yppandeförbud 4) uppskjutande av en anmälan som avses i 44 § 1 mom. (2 mom.).

I slutet av polislagens 5 a kap. regleras bemyndigandet att utfärda förordning (62 §) som indelas i ärenden som regleras genom förordning av statsrådet och genom förordning av inrikesministeriet.

Lag om civil underrättelseinhämtning avseende datatrafik

Föremål för underrättelseinhämtning som avser datatrafik

I lagen föreskrivs det om användning av underrättelseinhämtning som avser datatrafik i civil underrättelseverksamhet. En användare i underrättelseinhämtning som avser datatrafik som avses i lagen är skyddspolisen som fungerar som civil underrättelsemyndighet.

Handlingar som allvarligt hotar den nationella säkerheten och som skyddspolisen får inhämta information om genom underrättelseinhämtning som avser datatrafik räknas uttömmande upp i lagen. De grundläggande hoten i underrättelseinhämtning som avser datatrafik är de samma som för metoderna för underrättelseinhämtning i polislagens 5 a kap. Därmed säkerställs det att den civila underrättelseverksamheten är en ändamålsenlig och effektiv helhet som består av olika metoder för underrättelseinhämtning. Eftersom informationen som fås genom underrättelseinhämtning som avser datatrafik är tänkt att fungera som input vid användning av de metoder för underrättelseinhämtning som avses i polislagens 5 a kap. möjliggör samma innehåll i fråga om de grundläggande hoten att man kan övergå till att använda de andra metoderna för underrättelseinhämtning tillräcklig smidigt och i tillräcklig omfattning.

De grundläggande hot som är föremål för underrättelseinhämtning som avser datatrafik är de samma som i polislagens 5 a kap. 3 §.

Allmän beskrivning av underrättelseinhämtning som avser datatrafik

Med underrättelseinhämtning som avser datatrafik avses enligt lagens 2 § teknisk informationsinhämtning riktad mot datatrafik i kommunikationsnät som överskrider Finlands gräns, vilken baserar sig på automatiserad avskiljning av datatrafiken samt behandling av den inhämtade informationen. Underrättelseinhämtning som avser datatrafik gäller på så sätt enbart datatrafik som överskrider rikets gräns genom överföring från ett finländskt kommunikationsnät till ett utländskt kommunikationsnät eller tvärtom. En betydande del av den finländska datakommunikationen avgränsas redan på denna nivå av grundläggande slag från underrättelseinhämtning som avser datatrafik.

Underrättelseinhämtning som avser datatrafik används på datatrafik i kommunikationsnät som överskrider gränsen. I definitionen av kommunikationsnät ingår ett krav på dataöverföringens elektromagnetiska utförande, men i övrigt är den teknologineutral till karaktären. Eftersom merparten av datatrafiken mellan Finland och andra länder förmedlas i kablar som använder optisk fiber för dataöverföring riktas underrättelseinhämtning som avser datatrafik i praktiken

huvudsakligen mot datatrafik som förmedlas via kablar. Med begreppet teknologineutral för kommunikationsnät säkerställs det emellertid att lagen kan tillämpas även i andra tekniska miljöer och i föränderliga kommunikationsteknologiska förhållanden.

Underrättelseinhämtning som avser datatrafik grundar sig som metod på automatiserad avskiljning av datatrafiken. Det särskiljer den från andra metoder för underrättelseinhämtning som riktas mot elektronisk kommunikation såsom teleavlyssning och teleövervakning. Det är inte fråga om informationsinhämtning som riktas mot en enskild teleadress eller teleterminalutrustning som man känner till utan om filtrering av datakommunikation som sker med automatiska metoder på en sådan punkt i ett kommunikationsnät genom vilket man kan anta att datatrafik som har samband med ett hot som ska utredas rör sig. En lösning som grundar sig på filtrering av datatrafik gör det möjligt att upptäcka kommunikation som har samband med ett hot och identifiering och lokalisering av aktörer i bakgrunden. Filtreringen genomförs genom att jämföra utvalt dataflöde med kriterier som på förhand satts upp som sökbegrepp.

Filtreringen ska inte i något enskilt fall av användning av underrättelseinhämtning som avser datatrafik omfatta all den datatrafik som överskrider Finlands gränser i kommunikationsnät. Användning av underrättelseinhämtning som avser datatrafik förutsätter att skyddspolisen har vetskap eller misstankar om den konkreta existensen av ett grundläggande hot och dess realiteter. Hotets respektive karaktär och de faktum man känner till om det påverkar i vilken del av kommunikationsnätet man kan anta att hotkommunikationen överskrider Finlands gräns. Främmande statliga aktörers datatrafik kan till exempel antas överskrida gränsen i andra delar av kommunikationsnätet än utbyte av meddelanden som har samband med terroristisk verksamhet som försiggår mellan Finland och konfliktområden.

Det förutsätts att den del av kommunikationsnätet som överskrider gränsen där sökbegreppen kan användas på datatrafiken nämns i skyddspolisens yrkande om tillstånd för underrättelseinhämtning som avser datatrafik och i domstolens beslut om tillstånd. Sökbegreppen får inte användas på datatrafik som rör sig i andra delar av kommunikationsnätet än de som nämns i tillståndet. Hur omfattande delen av kommunikationsnätet som överskrider gränsen det i vart och ett fall ska vara nödvändigt att använda sökbegreppen på beror bland annat på hotets karaktär och på de kommunikationsmetoder personerna i bakgrunden för hotet antas använda.

I lagen regleras de metoder som är nödvändiga för att få uppgifter som påverkar valet av en del av kommunikationsnätet för kravet på tillstånd. Skyddspolisen ska ges rätt att ge försvarsmaktens underrättelsetjänst uppdrag om utredning av detta. Utredningsverksamheten hos försvarsmaktens underrättelsetjänst grundar sig på statistisk analys av dataflöden. Detaljerna för befogenheten som gäller den statistiska analysen och det tillståndsförfarande som behövs ska finnas i lagen om militär underrättelseverksamhet. Därefter regleras en skyldighet för ägare till och innehavare av kommunikationsnät att ge skyddspolisen uppgifter som de innehar och som är nödvändiga för valet av kommunikationsnät.

Genomförandet av underrättelseinhämtning som avser datatrafik kräver att det på förhand byggts anslutningar för den del av kommunikationsnätet som överskrider gränsen. Anslutningarna byggs under medverkan av de företag som äger eller innehar den del av kommunikationsnätet som överskrider gränsen. När tillstånd för underrättelseinhämtning som avser datatrafik har erhållits av domstolen görs kopplingen i kommunikationsnätet enligt tillståndet. Genom kopplingen styrs den datatrafik som rör sig i kommunikationsnätet enligt tillståndet till filtrering. Suomen Erillisverkot Oy utför kopplingen och överlåter datatrafiken enligt tillståndet. Uppgiften ska anvisas till en aktör som är oberoende av underrättelsemyndigheterna för att säkerställa att de inte får mer omfattande tillträde till datatrafiken än det som tillåts i domstolens tillståndsbeslut.

Datatrafiken som kopplas av Suomen Erillisverkot Oy ska speglas så att den flödar genom det system för teknisk underrättelseinhämtning som försvarsmaktens underrättelsetjänst administrerar. Försvarsmaktens underrättelsetjänst åläggs i lagen att vara teknisk utförare för skyddspolisens underrättelseinhämtning som avser datatrafik. Riktandet av underrättelseinhämtning som avser datatrafik mot datatrafik i kommunikationsnät behandlas mer ingående nedan i avsnittet om informationssamhället.

Sökbegreppen som godkänts i domstolens tillståndsbeslut ska på förhand matas in i systemet för underrättelseinhämtning, och systemet jämför automatiserat datatrafiken som strömmar igenom med dem. Den automatiserade jämförelsen sker i realtid. Den trafik som motsvarar sökbegreppen styrs åt sidan för fortsatt behandling medan datatrafik som inte motsvarar sökbegreppen fritt strömmar genom systemet. Den trafik som inte motsvarar sökbegreppen ska efter genomströmningen inte gå att återställa för att undersökas av underrättelsemyndigheterna.

Försvarsmaktens underrättelsetjänst vidarebefordrar datatrafiken som motsvarar sökbegreppen till skyddspolisen. Denna datatrafik som i princip är relevant för utredningen av ett grundläggande hot genom underrättelseinhämtning som avser datatrafik kan behandlas automatiskt och manuellt. I behandlingen får skyddspolisen utreda innehåll och övriga uppgifter i enskilda konfidentiella meddelanden.

Skyddspolisens rätt att registrera uppgifter som inhämtats med hjälp av underrättelseinhämtning som avser datatrafik i sitt funktionella informationssystem på samma sätt som utplåning av registrerade uppgifter och utlämnande från informationssystem fastställs enligt bestämmelserna i polisens personuppgiftslag. Lagen om civil underrättelseinhämtning avseende datatrafik ska dock innehålla en del bestämmelser om behandling av personuppgifter som bör tillämpas redan innan bedömningen av förutsättningen för registrering av information. Bestämmelserna gäller särskilda så kallade förbud mot underrättelseinhämtning som avser begränsning av användningen av datatrafik, granskning och undersökning av upptagningar och handlingar som samlats, skyldighet att utan dröjsmål utplåna vissa uppgifter som erhållits och utlämnande av uppgifter som erhållits genom underrättelseinhämtning som avser datatrafik. Förbuden mot underrättelseinhämtning och skyldigheterna att utplåna som föreslås i lagen begränsar betydligt vilka uppgifter som genom underrättelseinhämtning som avser datatrafik som får registreras i skyddspolisens funktionella informationssystem.

Sökbegrepp som får användas i underrättelseinhämtning som avser datatrafik

Av bedömningen av nuläget (metoder för inhämtande av information ur telenät nedan) framgår det att i verksamhet som kan karaktäriseras som underrättelseinhämtning som avser datatrafik kan datatrafik filtreras både med hjälp av sökbegrepp som framför allt beskriver innehållet i ett meddelande och sökbegrepp som riktas mot datatrafikens övriga uppgifter. Användning av sökbegrepp som beskriver innehåll i meddelanden kan anses innehålla ett mer ingående ingripande i utomståendes konfidentiella kommunikation, för verksamheten kräver datatekniskt öppnande av all kommunikation som omfattas av filtreringen för utredning av om innehållet motsvarar sökbegreppet. Ett meddelandes innehåll har traditionellt ansetts utgöra kärnområdet för konfidentiella meddelandens hemlighet.

Bestämmelser om sökbegrepp ska ingå i lagens 4 §. Användning av sökbegrepp som beskriver innehållet i konfidentiella meddelanden ska vara totalt förbjudet i underrättelseinhämtning som avser datatrafik. Uttryck eller personers namn- eller övriga identifieringsuppgifter som hör till meddelandets semantiska innehåll ska således inte alls få användas som sökbegrepp. Det gäller en betydande begränsning som sätts för underrättelseverksamheten med syftet att så långt som möjligt skydda kommunikationshemlighetens kärnområde för personer i utomstå-

ende ställning. I de jämförelseländer som har lagstiftning om underrättelseinhämtning som avser datatrafik har motsvarande begränsningar eller hinder mot att använda innehållsliga sökbegrepp inte ställts upp, utan det är i vid utsträckning tillåtet att använda dem i de länderna.

Tillåtna övriga sökbegrepp än uppgifter som beskriver konfidentiella meddelandens semantiska innehåll är framför allt styr- och förmedlingsuppgifter för datatrafiken, det vill säga sådana instruktioner, kommandon och övriga metadata till datanätet eller till det sändande eller mottagande datasystemet genom vilka man påverkar transporten och styrningen av ett meddelande i kommunikationsnät och informationssystem. Uppgifter som tillåts som sökbegrepp är även till exempel uppgifter om användningen av ett krypteringsprogram eller en alfabetisk teckenuppsättning.

All kommunikation åtnjuter inte skydd av hemligheten i ett konfidentiellt meddelande. Av den orsaken ska lagens 4 § 2 mom. tillåta att ett sökbegrepp som beskriver ett meddelandes semantiska innehåll används i två undantagsfall. Ett sökbegrepp som beskriver innehåll får för det första användas när underrättelseinhämtning som avser datatrafik kan riktas enbart mot en främmande stats eller en jämförbar aktörs datatrafik. Tillämpning av undantaget ska komma på fråga endast om det i det dataflöde där sökbegreppen används inte finns någon utomstående kommunikation som skyddas av hemligheten i konfidentiella meddelanden.

Det andra undantaget gäller skadliga datorprogram eller kommandon. Sökbegreppen som beskriver innehållet i ett skadligt datorprogram eller kommando är olika tekniska teckenkombinationer och inte ord eller uttryck ur ett mänskligt språk. På grund av den särskilda karaktären för sökbegrepp som gäller skadliga datorprogram kan de också jämföras med innehållet i meddelanden som omfattas av kommunikationshemligheten. Lösningen är till den delen såväl tekniskt sett som i sak den samma som i 272 § i lagen om tjänster inom elektronisk kommunikation.

Sökbegreppen som används i underrättelseinhämtning som avser datatrafik får inte fritt formuleras av skyddspolisen. Innan verksamhet inleds ska de ha specificerats och godkänts i domstolens tillståndsbeslut om underrättelseinhämtning som avser datatrafik (7 §), eller, undantagsvis, genom ett brådskande beslut av chefen för skyddspolisen (9 §).

Enligt 7 § kan domstolen i sitt tillståndsbeslut utöver enskilda sökbegrepp även godkänna kategorier av sökbegrepp. Skyddspolisen tillåts att själv bilda sökbegrepp som ska användas i underrättelseinhämtning som avser datatrafik inom ramen för kategorin för de sökbegrepp som domstolen godkänner. Förslaget grundar sig på betänkandet av arbetsgruppen för en informationsanskaffningslag enligt vilken man för att kunna rikta datatrafikspaningen vid sidan av sökbegrepp som har definierats tillräckligt exakt på förhand också bör kunna använda ”beskrivningar i ord av den verksamhet som äventyrar den nationella säkerheten och som så konkret som möjligt karaktäriserar föremålet för informationsinhämtningen.” Föremål för beskrivningen ska vara sådana kommunikationsmässiga och andra verksamhetsmodeller som man vet eller som man kan anta att har samband med verksamhet som äventyrar den nationella säkerheten (s. 65).

Enligt uppfattningen i arbetsgruppen för en informationsanskaffningslag kan ett tillståndsförfarande som grundar sig på godkännandet av kategorier av sökbegrepp anses uppfylla de krav som Europeiska människorättskonventionen ställer. I lagstiftningen i Sverige och i Schweiz anges godkännandet av kategorier av sökbegrepp som grund för datatrafikspaning på motsvarande sätt som det som föreslås här. Vid utarbetandet av en lag om underrättelseinhämtning för Schweiz kunde man beakta Europeiska människorättsdomstolens senaste beslutspraxis.

Med kategori av sökbegrepp i lagen som föreslås avses en skarpt avgränsad verbal beskrivning av sökbegrepp som är relevanta för frågan om underrättelseinhämtning. Man ska kunna söka tillstånd för en kategori av sökbegrepp i en situation där en grupp sinsemellan jämförbara sökbegrepp som hör till samma klara helhet av vilka endast en del är kända när underrättelseinhämtning som avser datatrafik inleds.

Eftersom domstolens godkännande av tillstånd om kategorier av sökbegrepp gäller att ge skyddspolisen begränsad rätt att själv formulera konkreta sökbegrepp som ska användas i underrättelseinhämtning som avser datatrafik kräver verksamheten särskild övervakning. Föremålet för övervakningen är att de konkreta sökbegreppen formuleras inom kategorin för sökbegrepp som nämns i domstolens tillståndsbeslut. Bestämmelser om övervakningen ingår i justitieministeriets förslag till lag om övervakning av underrättelseinhämtning som finns i denna proposition (/).

Allmänna förutsättningar för användning av underrättelseinhämtning som avser datatrafik

De allmänna förutsättningarna för underrättelseinhämtning som avser datatrafik regleras i lagens 4 §. Förutsättningen för all underrättelseinhämtning som avser datatrafik är att verksamhetens resultat motiverats. Enbart en motiverad förväntan på resultat lämpar sig när underrättelseinhämtning som avser datatrafik kan riktas endast mot en statlig eller en därmed jämställbar aktörs datatrafik. Med en aktör som är jämställbar med en statlig avses en aktör vars struktur liknar en stats struktur och som på ett bestämt område använder egen och permanent makt. Tillämpning av enbart motiverade förväntade resultat grundar sig på att stater och aktörer som är jämställbara med dem inte åtnjuter kommunikationshemlighet.

I andra fall är den allmänna förutsättningen för att underrättelseinhämtning som avser datatrafik utöver att den ska ge resultat att den är nödvändig, vilket är den högsta tröskeln för förutsättningar som lagstiftningen om polisens befogenhet känner. Förutsättningen om nödvändighet tillämpas i de fall där objektet för underrättelseinhämtning som avser datatrafik i sig är en främmande stat, men användningen av sökbegrepp omfattar även annan datakommunikation, och de fall där objektet för underrättelseinhämtning som avser datatrafik åtnjuter hemlighet i konfidentiella meddelanden.

För underrättelseinhämtning som avser datatrafik sätts strängare villkor än för de metoder för underrättelseinhämtning som riktas mot kommunikation och som föreslås i polislagens 5 a kap. I bakgrunden för lösningen finns Europeiska människorättsdomstolens avgörande i fallet Szabo & Vissy mot Ungern enligt vilket användningen av underrättelseinhämtning som avser datatrafik på ett allmänt plan bör vara ovillkorligen nödvändig för att skydda demokratiska institutioner, och i samband med en enskild underrättelseoperation ovillkorligen nödvändig för att få väsentligen viktig information. De föremål för underrättelseinhämtning som avser datatrafik som specificeras i 3 § riktas mot demokratin och dess centrala institutioner, och då kan underrättelseinhämtningen som avser datatrafik gälla användningen av en nödvändig befogenhet för att skydda demokratin. Genom att föreskriva att förutsättningen för underrättelseinhämtning som avser datatrafik är nödvändig svarar man på kravet att användningen av underrättelseinhämtning som avser datatrafik i enskilda fall ska vara ovillkorligen nödvändig. Det är svårt att se någon avgörande skillnad mellan människorättsdomstolens ”ovillkorligen nödvändig” och den högsta tröskeln ”nödvändig” i den nationella lagstiftningen om befogenheter. Även i Sveriges och Schweiz lagstiftning har nödvändighet ställts som tröskel för förutsättningen.

Med kravet att underrättelseinhämtning som avser datatrafik ska vara nödvändig avses att den ska användas i sista hand, det vill säga att det är omöjligt eller oskäligt svårt att inhämta uppgifter på annat sätt. Tillämpningen av kravet förutsätter att såväl skyddspolisen som yrkar på

tillstånd för underrättelseinhämtning som avser datatrafik som domstolen som beslutar om yrkandet om tillstånd jämför å ena sidan metoderna som avses i polislagens 5 a och å andra sidan underrättelseinhämtning som avser datatrafik. Om det inte är omöjligt eller oskäligt svårt att använda de andra metoderna för underrättelseinhämtning bör de användas som primära metoder i förhållande till underrättelseinhämtning som avser datatrafik. I lagens 4 § 3 mom. finns en bestämmelse som preciserar kravet på nödvändighet och som gör den ännu strängare i förhållande till metoderna för informationsinhämtning ur telenät enligt vilken identifieringsuppgifter för teleterminalutrustning eller teleadresser inte alls får användas som sökbegrepp för underrättelseinhämtning som avser datatrafik i Finland. Om skyddspolisen innehar sådan information får den över huvud taget inte använda underrättelseinhämtning som avser datatrafik, utan den bör använda teleavlyssning, teleövervakning eller övriga befogenheter för informationsinhämtning ur telenät som föreslås i 5 a kap. i polislagen.

Beslutsfattande om underrättelseinhämtning som avser datatrafik

Europeiska människorättsdomstolen har ansett det vara en viktig garanti för rättssäkerheten att en domstol eller en annan myndighet som verkställer juridisk prövning beslutar om åtgärder som ingriper i skyddet av konfidentiella meddelanden. Det räcker dock inte att den formella beslutanderätten hör till en domstol, utan den nationella lagen ska dessutom innehålla tillräckliga kriterier som styr domstolens tillståndsprövning. Av lagen ska med tillräcklig noggrannhet framgå de hot för vilka domstolen kan bevilja tillstånd för informationsinhämtning, och grunderna för hur informationsinhämtningen riktas mot en person bör framgå. Den som ansöker om tillstånd ska motivera sin ansökan och lägga fram tillräcklig information om de faktum som stöder den. Dessutom ska bland annat giltighetstiden för informationsinhämtningen framgå tillräckligt entydigt av domstolens beslut.

Arbetsgruppen för en informationsanskaffningslag ansåg att tillståndsprövningen bör vara juridisk till sin art. Dessutom konstaterade arbetsgruppen att när tillståndsförfarandet ordnas bör offentlighets- och sekretessfaktorer, behovet av specialkunnande som frågorna kräver samt säkerställandet av individens rättsskydd beaktas (s. 69). Med att konstatera behovet att beakta specialkunnande torde arbetsgruppen ha hänvisat till möjligheten att grunda en specialdomstol för uppgiften.

Enligt lagens 7 § beslutar domstolen om ärenden som gäller underrättelseinhämtning som avser datatrafik på skriftligt yrkande av chefen för skyddspolisen. Enligt 8 § ska vid behandling och vid avgörande i domstol av tillståndsärenden bestämmelserna om tillståndsärenden som gäller metoder för underrättelseinhämtning i 5 a kap. 35 § i polislagen iakttas. Enligt bestämmelsen som det hänvisas till är Helsingfors tingsrätt forum för underrättelseinhämtning som avser datatrafik. Eftersom Helsingfors tingsrätt också i övrigt har den bredaste erfarenheten i landet av behandling av ärenden som gäller hemlig informationsinhämtning och tvångsmedel kan det specialkunnande som arbetsgruppen för en informationsanskaffningslag förutsätter uppnås genom att koncentrera de ärenden som gäller underrättelseinhämtning som avser datatrafik till den.

Lagens 7 § ska innehålla en detaljerad förteckning över de omständigheter som ska framgå av skyddspolisens yrkande om tillstånd att använda underrättelseinhämtning som avser datatrafik och av Helsingfors tingsrätts beslut. Förebilden för förteckningen är bestämmelserna om beslutsfattandet i ärenden som gäller användning av metoder för informationsinhämtning ur telenät i polislagens 5 kap. Förteckningen innehåller tillräckliga kriterier som styr domstolens tillståndsprövning och som Europeiska människorättsdomstolen förutsätter. Det förutsätts att föremålet som är grund för underrättelseinhämtning som avser datatrafik och de faktum som gäller föremålet samt de faktum som förutsättningarna för användning av underrättelseinhämtning som avser datatrafik grundar sig på, till exempel ett allvarligt hot mot den nationella

säkerheten och nödvändighet, framgår av yrkandet om tillståndet och av beslutet. Beviljandet av tillstånd förutsätter att domstolen utgående från det material som skyddspolisen lägger fram blir övertygad om de ovan nämnda omständigheterna.

I yrkandet och beslutet om tillstånd ska det redogöras också för flera andra saker, bland annat om de sökbegrepp som ska användas i verksamheten eller deras kategorier med motivering för dem, den kommunikationsnätsdel som överskrider gränsen i fråga om sökbegrepp som används, exakt giltighetstid för tillståndet och den tjänsteman som ansvarar för övervakningen av underrättelseinhämtning som avser datatrafik. Domstolen ska ha möjlighet att i sitt beslut sätta gränser och villkor för användningen av underrättelseinhämtning som avser datatrafik. Domstolens beslut sätter sammantaget noggranna gränser för på vilket sätt och i vilken omfattning skyddspolisen får genomföra underrättelseinhämtning som avser datatrafik i varje enskilt fall.

Tillstånd för underrättelseinhämtning som avser datatrafik ska beviljas för högst 6 månader. Av avsnittet i betänkandet som beskriver internationell rättspraxis framgår det att Europeiska människorättsdomstolen har ansett att denna giltighetstid är ändamålsenlig. I lagstiftningen i Sverige och Schweiz har likaså den maximala giltighetstiden fastställts till 6 månader.

Användningen av underrättelseinhämtning som avser datatrafik ska oberoende av den nämnda tidsfristen avslutas om syftet med den har nåtts eller om det inte längre finns förutsättningar för den.

För så kallade brådskande situationer är det motiverat att lägga till en möjlighet till lättare beslutsförfarande. Europeiska människorättsdomstolen har ansett att den nationella lagen kan innehålla specialbestämmelser om beslutsförfarande för brådskande situationer under förutsättning att det framgår av lagen att det får användas endast undantagsvis och av nödvändiga skäl. Om det föreskrivs om avvikande beslutsförfarande ska det också föreskrivas om den normala beslutsfattarens möjlighet att i efterhand bedöma om förfaringssättet var motiverat. På samma sätt ska det föreskrivas om utplåning av de uppgifter som fåtts med stöd av ett omotiverat brådskande beslut.

Beslutsförfarandet i brådskande situationer regleras i enlighet med de ovannämnda kvalitetskraven. Chefen för skyddspolisen ska enligt 8 § fatta beslut i brådskande situationer. Förfarandet ska komma i fråga endast om ett ärende inte tål uppskov, det vill säga om en fördröjning som det normala tillståndsförfarandet orsakar allvarligt hotar den nationella säkerheten. Det kan antingen gälla en situation med ett omedelbart hot eller en situation där fördröjningen som orsakas av ansökan om tillstånd leder till att material som kan fås genom underrättelseinhämtning oåterkalleligen förloras.

Ett brådskande beslut som chefen för skyddspolisen fattat gäller endast tills domstolen har avgjort om yrkandet på tillstånd ska beviljas. Ett brådskande beslut ska föras till domstolen för bedömning senast 24 timmar efter det att den underrättelseinhämtning som avser datatrafik inleddes. Utplåning av information som visar sig vara omotiverad och som inhämtats med hjälp av ett brådskande beslut behandlas nedan i samband med förbud mot underrättelseinhämtning och skyldighet till utplåning. I praktiken bör fattandet av brådskande beslut bli marginellt.

Tekniskt genomförande av underrättelseinhämtning som avser datatrafik

Underrättelseinhämtning som avser datatrafik ska regleras i två olika lagar om befogenhet. Skyddspolisens rätt att använda information om föremål för underrättelseinhämtning som avser datatrafik som inhämtats på detta sätt regleras i lagen om civil underrättelseinhämtning avseende datatrafik. Försvarsmaktens rätt att använda underrättelseinhämtning som avser data-

trafik för att inhämta information om militär och övrig verksamhet regleras i lagen om militär underrättelseverksamhet.

När det finns två myndigheter som har rätt att använda underrättelseinhämtning som avser datatrafik är det möjligt att organisera verksamheten separat för båda förvaltningsområdena eller alternativt gemensamt för att uppnå synergifördelar. Arbetsgruppen för en informationsanskaffningslag ansåg att det tekniska utförandet av datatrafikspaningen bör grundas på en centraliserad lösning där en myndighet inhämtar de uppgifter genom datatrafikspaning som de andra myndigheterna behöver (s. 67). Lösningen motiveras framför allt av kostnadssynpunkter. Ur resurssynvinkel är det inte förnuftigt att skyddspolisen och försvarsmakten bygger upp egna tekniska system och lösningar för samma funktion. Också kraven som ställs på att funktionen är enhetlig, på den specialisering funktionen kräver och på aspekter som gäller laglighetsövervakningen motiverar att det tekniska genomförandet av underrättelseinhämtning som avser datatrafik som uppgift ges en myndighet. Arbetsgruppen för en informationsanskaffningslag bedömde att försvarsmaktens underrättelsetjänst lämpar sig bäst som ansvarig myndighet för det tekniska genomförandet (s. 68).

Enligt vad som sägs ovan anvisas det tekniska genomförandet av underrättelseinhämtning som avser datatrafik försvarsmaktens underrättelsetjänst. Den ska ansvara för det tekniska kunnande som underrättelseinhämtningen kräver och för byggandet och förvaltningen av de tekniska systemen också för den civila underrättelseverksamhetens behov.

Det viktigaste innehållet i det tekniska genomförandet är att försvarsmaktens underrättelsetjänst utför avskiljning av datatrafiken för skyddspolisen. Skyddspolisens rätt att ge uppdrag som gäller detta anges i 10 § 3 mom. i lagen som föreslås. I praktiken ordnas verksamheten så att skyddspolisen lämnar tillståndsbeslutet om underrättelseinhämtning som avser datatrafik till underrättelsetjänsten. Av tillståndsbeslutet framgår bland annat de sökbegrepp som får användas i filtreringen och den del av kommunikationsnät som filtreringen får gälla. Suomen Erillisverkot Oy som ansvarar för kopplingen som underrättelseinhämtning som avser datatrafik kräver överlåter den datatrafik som rör sig i en kommunikationsnätsdel enligt tillståndet till försvarsmaktens underrättelsetjänst, som speglar den att flöda genom det tekniska system för underrättelseinhämtning som den förvaltar. Försvarsmaktens underrättelsetjänst ska på förhand ha matat in sökbegreppen som framgår av tillståndsbeslutet i systemet för underrättelseinhämtning. Försvarsmaktens underrättelsetjänst levererar datatrafiken som avskiljts med hjälp av användning av sökbegreppen till skyddspolisen som är uppdragsgivare. Den fortsatta behandlingen av den avskiljda datatrafiken som det föreskrivs om i 5 § är inte en del av det tekniska genomförandet av underrättelseinhämtning som avser datatrafik varvid endast skyddspolisen ansvarar för utförandet och lagenligheten.

Domstolen kan i tillståndet den beviljar skyddspolisen tillåta att, förutom sökbegrepp, även kategorier av sökbegrepp används. Formulerandet av konkreta sökbegrepp inom ramen för en kategori som definierar sökbegrepp är inte en del av tekniska genomförandet utan endast skyddspolisen ansvarar för det. Skyddspolisen levererar till försvarsmaktens underrättelsetjänst endast sådana sökbegrepp som den som sådana kan mata in i systemet för underrättelseinhämtning att använda för filtrering.

Det tekniska genomförandet inbegriper utöver filtrering av datatrafik också åtgärder som möjliggör senare underrättelseinhämtning som avser datatrafik. Avsikten med dem är att för ett yrkande om tillstånd inhämta information om i vilken kommunikationsnätsdel underrättelseinhämtning som avser datatrafik kommer att användas. Föregripande specificering av en kommunikationsnätsdel är relevant för att det inte ska komma in onödig utomstående datatrafik som omfattas av användningen av sökbegreppen.

I 10 § 2 mom. i lagförslaget anges skyddspolisens rätt att ge försvarsmaktens underrättelsetjänst i uppdrag att behandla tekniska data i enlighet med 66 § i lagen om militär underrättelseverksamhet. Den aktuella paragrafen i lagen om militär underrättelseverksamhet tillåter underrättelsetjänsten att tillfälligt samla in teknisk information om ett kommunikationsnäts datatrafik och analysera den statistiskt för att utreda i vilken kommunikationsnätsdel datatrafik som har samband med en viss hotande aktivitet mest sannolikt rör sig. Behandling av teknisk information förutsätter enligt 67 § i lagen om militär underrättelseverksamhet tillstånd av domstol. Försvarsmaktens underrättelsetjänst ansöker om tillståndet också när det är frågan om verksamhet som sker på uppdrag av skyddspolisen. I yrkandet om tillstånd för behandling av teknisk information krävs det att man lägger fram sådana omständigheter som gäller verkställandet av ett tillstånd som den som i praktiken ordnar saken har den bästa informationen om, det vill säga försvarsmaktens underrättelsetjänst.

När den statistiska analysen är klar levererar försvarsmaktens underrättelsetjänst resultatet av den till skyddspolisen. Resultatet av den statistiska analysen innehåller inte information som omfattas av kommunikationshemligheten. Utifrån resultatet kan skyddspolisen bedöma för vilken kommunikationsnätsdel den bör ansöka om tillstånd för underrättelseinhämtning som avser datatrafik av domstolen.

Identifieringen av en kommunikationsnätsdel för tillståndsansökningen förutsätter oftast utöver de åtgärder av försvarsmaktens underrättelsetjänst som beskrivs ovan även att skyddspolisen får vissa uppgifter som innehas av företag som äger eller innehar kommunikationsnät. Företagens skyldighet att lämna uppgifter behandlas nedan.

Förbud mot underrättelseinhämtning och skyldigheter att utplåna information

På grund av att underrättelseinhämtning som avser datatrafik skiljer sig från andra underrättelseinhämtningsmetoder föreslås det bestämmelser om särskilda förbud mot att rikta underrättelseinhämtning som avser datatrafik mot vissa typer av meddelanden och uppgifter. Trots dessa förbud kan det vid underrättelseinhämtning som avser datatrafik komma fram meddelanden och uppgifter som omfattas av förbudet mot underrättelseinhämtning. Förbudet mot underrättelseinhämtning ska därför förstärkas genom bestämmelser om skyddspolisens skyldighet att utan dröjsmål utplåna sådana meddelanden och uppgifter som omfattas av förbudet då deras art har klarlagts. Skyldigheten att utan dröjsmål utplåna information gäller också vissa andra meddelanden och uppgifter än sådana som omfattas av förbudet mot underrättelseinhämtning.

De förbud mot underrättelseinhämtning som föreslås i lagen grundar sig i huvudsak på förslag från arbetsgruppen för en informationsanskaffningslag. Enligt arbetsgruppens betänkande skulle avsikten med underrättelseinhämtning som avser datatrafik inte vara att följa datatrafiken mellan parter som befinner sig i Finland och inte heller sådant sparande av information i en molntjänst utomlands som sker i Finland och som inte inbegriper kommunikation. Ifall det införs bestämmelser om underrättelseinhämtning som avser datatrafik bör det tillräckligt noggrant säkerställas att sådan här information omedelbart utplånas då den upptäcks (s. 68, på finska).

I den lag som föreslås finns det bestämmelser om förbud mot underrättelseinhämtning och skyldighet att utplåna information som gäller för kommunikation inom Finland, men inte några särskilda motsvarande bestämmelser som gäller för sparande av information i molntjänster. Orsakerna till att man gått in för en lösning som skiljer sig från arbetsgruppens ställningstagande behandlas i slutet av detta avsnitt.

Det förbud mot underrättelseinhämtning som gäller kommunikation inom Finland finns i 12 § i lagförslaget. Där föreskrivs det att underrättelseinhämtning som avser datatrafik inte får riktas mot kommunikation där både sändaren och mottagaren finns i Finland. Underrättelseinhämtning som avser datatrafik ska inte användas i det interna kommunikationsnätet i Finland utan enbart i det gränsöverskridande kommunikationsnätet i syfte att inhämta information om externa hot. Kommunikationen mellan en sändare och mottagare som båda befinner sig i Finland går ofta via ett gränsöverskridande kommunikationsnät. Bestämmelserna om förbud mot underrättelseinhämtning föreslås i syfte att säkerställa att all kommunikation som är avsedd att ske inom landet är likställd oavsett vilken rutt kommunikationen tar på grund av slumpmässiga faktorer.

Enligt 12 § i lagförslaget får underrättelseinhämtning inte heller riktas mot information där parterna i kommunikationen eller den som upptar kommunikationen har skyldighet eller rätt att vägra vittna med stöd av 17 kap. 13, 14, 16, 20 § eller 22 § 2 mom. i rättegångsbalken. Med stöd av bestämmelsen åtnjuter uppgifter skydd från underrättelseinhämtning som avser datatrafik om de omfattas av advokatsekretess, tystnadsplikt för yrkesutbildade personer inom hälso- och sjukvården, bikthemlighet för präster och källskydd för journalister. Förbudet mot underrättelseinhämtning ska inte gälla kommunikation i allmänhet mellan sådana yrkesutbildade personer som avses i rättegångsbalken, utan enbart de uppgifter som en person enligt rättegångsbalken uttryckligen har skyldighet eller rätt att inte vittna om.

Det är inte tekniskt möjligt att följa förbuden mot underrättelseinhämtning så att det inte alls skulle samlas in sådana uppgifter om datatrafiken som omfattas av förbuden. Sökbegreppen vid underrättelseinhämtning som avser datatrafik kan i allmänhet inte utformas så att de skulle kunna identifiera ett meddelande eller en uppgift som omfattas av förbudet mot underrättelseinhämtning och förhindra att informationen hamnar bland det material som styrs över till fortsatt behandling. Därför föreskrivs det i lagens 15 § om skyddspolisens skyldighet att utan dröjsmål utplåna sådana meddelanden och uppgifter som omfattas av förbudet mot underrättelseinhämtning då deras art har klarlagts. Skyldigheten att utplåna informationen ska vara absolut och det föreskrivs inte om några undantag. Av skyldigheten att utplåna informationen följer också ett absolut förbud mot att dra nytta av eller använda sådana här meddelanden eller uppgifter för något som helst ändamål.

I 15 § i lagförslaget föreskrivs det dessutom om skyddspolisens skyldighet att utan dröjsmål utplåna all sådan information som man har inhämtat genom underrättelseinhämtning som avser datatrafik och som inte behövs för att skydda den nationella säkerheten. Skyldigheten att utplåna information som är oväsentlig med tanke på skyddet av den nationella säkerheten är emellertid inte lika absolut som skyldigheten att utplåna meddelanden och uppgifter som omfattas av förbudet mot underrättelseinhämtning, utan de får under vissa villkor som det föreskrivs om särskilt överlämnas för brottsbekämpning och lagras i polisens personregister. Till exempel befogenheten att lagra information gäller endast om uppgifterna behövs för att utreda eller förhindra ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst sex år eller som en utredning som stöder det att någon är oskyldig.

Skyldigheterna att utplåna information stöds genom bestämmelser om skyldighet att utan ogrundat dröjsmål granska sådana upptagningar som gjorts i samband med underrättelseinhämtning som avser datatrafik (13 §). Upptagningar får undersökas enbart av sådana tjänstemän eller andra aktörer som nämns i lagen eller som särskilt förordnats eller anvisats denna uppgift (14 §).

En särskild bestämmelse gäller utplåning av information som inhämtats med stöd av ett ogrundat eller felaktigt beslut som fattats i en brådskande situation. Vid formuleringen av bestämmelsen har Europadomstolens avgörandepraxis beaktats. Om en domstol i sin bedömning

av ett beslut som fattats i en brådskande situation anser att de förutsättningar vad gäller resultat och nödvändighet som föreskrivits för underrättelseinhämtning som avser datatrafik inte har uppfyllts, ska enligt 9 § 2 mom. i lagförslaget allt det material som inhämtats genom sådan underrättelseinhämtning genast utplånas. Om domstolen anser att ett sådant här beslut till någon mindre del är felaktigt, ska informationen utplånas till den del som domstolens avgörande förutsätter det. En mindre felaktighet kan gälla till exempel ett sökbegrepp som är felformulerat, vilket innebär att information som inhämtats med hjälp av sökbegreppet i denna form måste utplånas. Undantag från regeln att information som inhämtats med stöd av ett ogrundat eller felaktigt beslut i en brådskande situation ska utplånas får göras endast om uppgifterna behövs för att utreda eller förhindra ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst sex år eller som en utredning som stöder det att någon är oskyldig. Det kan anses att det finns ett särskilt vägande samhälleligt intresse av att sådan information registreras och används.

Arbetsgruppen för en informationsanskaffningslag föreslog i sitt betänkande att förbudet mot underrättelseinhämtning och skyldigheten att utplåna information skulle gälla då en person i Finland sparar information som inte inbegriper kommunikation i en molntjänst utomlands. Ståndpunkten motiveras inte i betänkandet och motivet för den är inte känt. Bestämmelser om ett sådant här förbud mot underrättelseinhämtning finns inte i lagstiftningen i någon annan av de jämförelsestater som har behandlats i denna proposition och det föreslås inte att det tas in i den finländska lagstiftningen heller.

Ett viktigt syfte med underrättelseinhämtning som avser datatrafik är att upptäcka allvarliga hot mot den nationella säkerheten och att identifiera de personer som ligger bakom dem. Betydelsen av underrättelseinhämtning som avser datatrafik som riktas mot information som sparas i molntjänster är jämförbar med annan underrättelseinhämtning som avser datatrafik med avseende på detta syfte. Molntjänster används i själva verket i stor utsträckning i olika former av verksamhet som är kopplad till terrorism och spionage.

Underrättelseinhämtning som avser datatrafik behöver användas till exempel i situationer där man vet att planeringen och förberedandet av ett terrordåd sker i ett sådant begränsat grupparbetsutrymme som skapats i en molntjänst, men där de som är delaktiga i förberedelserna är okända. Trafiken från Finland till grupparbetsutrymmet kan upptäckas och personerna bakom den identifieras med hjälp av underrättelseinhämtning som avser datatrafik då man använder grupparbetsutrymmets position som sökbegrepp. Cyberspionage i statlig regi bedrivs i allmänhet så att de skadeprogram som används för spionage lagrar den stulna informationen i moln i utlandet. Om trafiken till molntjänster beläggs med ett förbud mot underrättelseinhämtning och skyldighet att utplåna information kan underrättelseinhämtning som avser datatrafik inte användas för att upptäcka och förhindra sådan här verksamhet.

Även andra faktorer talar mot ett förbud mot underrättelseinhämtning i anslutning till molntjänster, framför allt omöjligheten i att få fram en förnuftig begränsning av området för förbudet och en exakt definition av området. Bestämmelser om ett förbud mot underrättelseinhämtning skulle kräva att man definierar vad som avses med att spara information i en molntjänst. En definition kunde i princip utarbetas antingen utifrån tekniska aspekter eller utifrån den funktionella karaktären av sparande i molntjänster. Det första alternativet skulle stå i strid med den utgångspunkt som betonar teknikneutralitet som man i övrigt har gått in för i lagen. På grund av den allt snabbare utvecklingen inom informations- och kommunikationstekniken är det också sannolikt att en definition av sparandet i molntjänster som utgår från teknik mycket snabbt skulle föråldras, vilket skulle betyda att det förbud mot underrättelseinhämtning som är bundet till definitionen skulle förlora sin betydelse.

En teknikneutral definition som stöder sig på verksamhetens karaktär skulle däremot vara oexakt och oändamålsenlig. När man sparar information i en molntjänst är det fråga om att via nätet spara data på en server. En sådan definition skulle förutom säkerhetskopiering av data även omfatta till exempel en stor del av en www-tjänsts uppdateringar och användningen av sociala medietjänster, och underrättelseinhämtning som riktar sig mot sådana kan från fall till fall ha stor betydelse för upptäckten av allvarliga hot mot den nationella säkerheten. Ett förbud mot underrättelseinhämtning som är bundet till en definition som utgår från verksamhetens karaktär skulle också vara svårt att tillämpa i praktiken, eftersom det skulle förutsätta teknisk analys av varje datatrafikhändelse för att få reda på om händelsen utgjorde sådant sparande av information via nätet som överensstämmer med definitionen. Det finns inte heller någon saklig grund för att exempelvis sådan användning av sociala medier som grundar sig på sparande av data via nätet skulle behandlas på något annat sätt än annan användning av sociala medier.

Enligt förslaget från arbetsgruppen för en informationsanskaffningslag skulle sådant sparande i molntjänster som inbegriper kommunikation inte ha omfattats av det förbud mot underrättelseinhämtning som arbetsgruppen föreslog. Eftersom det i många fall torde vara omöjligt att skilja sådan här verksamhet från annat sparande i molntjänster skulle ett förbud och bestämmelser om undantag från förbudet leda till att området för förbudet skulle bli otydligt. Som ett exempel på molntjänsttrafik som inbegriper kommunikation kan man nämna en situation där en person som befinner sig i Finland sparar ett dokument i en molntjänst utomlands och där en person som befinner sig i ett annat land senare går in i tjänsten och läser dokumentet där. Eftersom den senare datatrafikhändelsen inte överskrider Finlands gräns i kommunikationsnätet, utan sker helt i utlandet, kan man inte göra några iakttagelser om den genom underrättelseinhämtning som avser datatrafik. Då förblir det oklart om det som har sparats i molntjänsten har inbegripit kommunikation eller inte och om förbudet mot underrättelseinhämtning är tillämpligt eller inte. De osäkerhetsfaktorer som är förknippade med tillämpningen av ett eventuellt förbud mot underrättelseinhämtning kan bedömas ha en försvagande verkan på rättssäkerheten.

Med anledning av det som sagts är det motiverat att underrättelseinhämtning som avser datatrafik ska få riktas in på sparande i molntjänster på samma villkor som när det gäller annan datatrafik. Ett sökbegrepp som gäller sparande i en molntjänst ska få användas om domstolen godkänner detta genom ett sådant beslut som avses i 7 §. Användningen av sökbegrepp som gäller sparande i en molntjänst ska alltid grunda sig på någon tillräckligt konkret verksamhet som är föremål för underrättelseinhämtning som avser datatrafik och som allvarligt hotar den nationella säkerheten. Skyddspolisen ska vara förpliktad att lämna fakta om verksamheten till domstolen i samband med yrkandet om tillstånd. Om användningen av ett sökbegrepp som gäller sparande i en molntjänst inte kan riktas in enbart på en främmande stats datatrafik och filtreringen även kan fånga in annan datatrafik, är förutsättningen för att sökbegreppet ska få användas i enlighet med 6 § 2 mom. att detta är nödvändigt.

Sökbegrepp för sådant som sparas i en molntjänst kan närmast vara information som beskriver var molntjänsten finns. Däremot får identifieringsuppgifter för teleadresser eller teleterminalutrustning som används av en person som befinner sig i Finland inte heller i detta fall användas som sökbegrepp, eftersom detta uttryckligen är förbjudet enligt lagens 4 § 3 mom. Följaktligen får underrättelseinhämtning som avser datatrafik inte användas till att inhämta information om all den data som har sparats i en utländsk molntjänst från en enskild känd enhet.

En fråga som är delvis separat från frågan om huruvida underrättelseinhämtning som avser datatrafik som uttryckligen gäller sparande i molntjänster ska tillåtas är huruvida datatrafik i anslutning till utomståendes personers användning av molntjänster får filtreras för sådan fortsatt behandling som avses i 5 §, och i så fall i vilken utsträckning, ifall de sökbegrepp som används vid filtreringen inte på något sätt ansluter sig till de utomståendes personernas trafik till

molntjänsten. Mera konkret kan man till exempel fråga sig hur sannolikt det är att utomstående datatrafik som gäller säkerhetskopiering av mobila enheter överensstämmer med ett sådant sökbegrepp baserat på uppgifter för styrning och förmedling av kommunikation som används för att utreda ett terrorhot. Enligt den bedömning som gjorts kan utomstående trafik till molntjänster endast i mycket exceptionella fall överensstämma med de sökbegrepp som får användas inom underrättelseinhämtning som avser datatrafik. Risken minskar genom den modell som valts för bestämmelserna, det vill säga att sökbegreppen inom underrättelseinhämtning som avser datatrafik inte får beskriva innehållet i ett meddelande.

Ifall utomstående trafik till en molntjänst ändå styrs över till fortsatt behandling ska samma bestämmelser om att information utan dröjsmål ska utplånas tillämpas som när det gäller annan datatrafik. I lagförslagets 13 § finns det bestämmelser om skyddspolisens skyldighet att utan ogrundat dröjsmål granska de upptagningar som uppkommit vid användningen av underrättelseinhämtning som avser datatrafik. Om man vid granskningen av upptagningar eller vid sådan undersökning av upptagningar som avses i 14 § hittar sådan information som saknar betydelse med avseende på skyddet av den nationella säkerheten, ska den enligt 15 § utan dröjsmål utplånas. Om information som har sparats i en molntjänst omfattas av till exempel advokatsekretess eller källskydd ska den dessutom utplånas utan dröjsmål oavsett om den hade haft betydelse för skyddet av den nationella säkerheten eller inte.

Skyldigheterna för privata företag

Det kommunikationsnät som överskrider Finlands gräns är i privat ägo. Därför förutsätter underrättelseinhämtning som avser datatrafik i praktiken att det föreskrivs om en tillräckligt omfattande skyldighet för dem som äger kommunikationsnätet att medverka till att underrättelseinhämtningen kan genomföras. Underrättelseinhämtningen kan till exempel inte genomföras om inte den datatrafik som löper genom kommunikationsnätet kan styras över från det privata nätet till det underrättelsesystem som drivs av försvarsmaktens underrättelsetjänst.

För de aktörer som omfattas av dessa skyldigheter används i lagen benämningen dataöverförare. Med dataöverförare avses enligt lagens 2 § en aktör som äger eller innehar en del av ett kommunikationsnät som överskrider Finlands gräns. Lagen ålägger inga andra privata aktörer än dataöverförare några skyldigheter. Det är skäl att betona att lagen inte ålägger företagen någon skyldighet att överlämna krypteringsnycklar till skyddspolisen eller att installera så kallade bakdörrar i sin programvara eller utrustning för skyddspolisens behov. Några sådana skyldigheter åläggs inte heller i lagen om militär underrättelseverksamhet, som innehåller kompletterande bestämmelser om det tekniska genomförandet av underrättelseinhämtning som avser datatrafik.

De skyldigheter som åläggs dataöverförare i denna lag och i lagen om militär underrättelseverksamhet är av två typer. För det första ska dataöverförare vara skyldiga att samarbeta vid byggandet av en sådan anslutning som underrättelseinhämtning som avser datatrafik kräver i den del av kommunikationsnätet som de äger eller innehar som överskrider gränsen. Existensen av en sådan anslutning är en förutsättning för att Suomen Erillisverkot Oy ska kunna göra en koppling i enlighet med domstolstillståndet och styra över sådan datatrafik som avses i tillståndet till försvarsmaktens underrättelsetjänst så att sökbegreppen kan användas. Skyldigheten att samarbeta då en anslutning ska byggas är nära kopplad till det tekniska genomförandet av underrättelseinhämtning som avser datatrafik och därför föreskrivs det om detta i lagen om militär underrättelseverksamhet.

Förutom den ovan nämnda samarbetsskyldigheten ska ägarna och innehavarna av kommunikationsnätet vara skyldiga att lämna skyddspolisen vissa uppgifter som är nödvändiga för det yrkande om tillstånd som ska framställas hos domstolen. Enligt 7 § i lagförslaget ska ett yr-

kande om tillstånd innehålla uppgifter om den del av ett kommunikationsnät som överskrider Finlands gräns där underrättelseinhämtning som avser datatrafik ska ske, samt en förklaring till varför denna del har valts. Det är motiverat att kommunikationsnätets del specificeras i yrkandet och beslutet om tillstånd så att den jämförelse utifrån sökbegrepp som görs inom underrättelseinhämtningen inte ska kunna riktas in på datatrafiken i större omfattning än vad som är nödvändigt för att utreda den verksamhet som allvarligt hotar den nationella säkerheten och som är föremål för underrättelseinhämtningen. Lagens 22 § ålägger på så sätt dataöverförarna skyldighet att lämna skyddspolisen sådana uppgifter som de innehar och som behövs för valet av den relevanta delen av kommunikationsnätet. Sådana uppgifter gäller framför allt reserveringar av överföringskapacitet som gjorts hos dataöverföraren, men även andra omständigheter som påverkar sannolikheten för vilken väg datatrafiken tar i den del av kommunikationsnätet som överskrider Finlands gräns. Däremot innebär paragrafen ingen skyldighet för dataöverförarna att lämna skyddspolisen information om enskilda kommunikationshändelser eller om parterna i sådana händelser.

Dataöverförarnas uppgiftsskyldighet tjänar samma syfte som den behandling av tekniska uppgifter som försvarsmaktens underrättelsetjänst utför för skyddspolisens räkning. Valet av metod eller kombination av metoder som ska användas för att med tanke på yrkandet om tillstånd identifiera den del av kommunikationsnätet som är relevant för underrättelseinhämtning som avser datatrafik kommer att variera från fall till fall. Målet är i vilket fall som helst att minimera risken för att utomstående datatrafik fångas in under underrättelseinhämtningen.

Dataöverföraren ska enligt 23 § ha rätt att få ersättning för direkta kostnader som orsakats av att överföraren har lämnat ut uppgifter. Rätten till ersättning, där skyddspolisen beslutar om utbetalningen, kommer att vara mera omfattande än när det gäller traditionella metoder för inhämtande av information ur telenät eftersom även personalkostnader kommer att ersättas som direkta kostnader.

Underrättelse om underrättelseinhämtning som avser datatrafik

Vid utformningen av bestämmelserna om underrättelse om underrättelseinhämtning som avser datatrafik har Europadomstolens avgörandepraxis beaktas. Europadomstolen har betonat rätten till effektiva rättsmedel mot lagstridig informationsinhämtning från myndigheternas sida för den som är föremål för informationsinhämtning. Förutsättningen för att rättsmedel ska kunna användas är i allmänhet att en person underrättas om myndighetsåtgärder som eventuellt kränker hens rättigheter. En myndighet ska på så sätt vara skyldig att på eget initiativ underrätta en person om informationsinhämtning som riktat sig mot personen då det inte längre finns något enskilt hinder för underrättelse. Om rätten att anföra klagomål över en myndighets informationsinhämtning emellertid är så allmänt formulerad i den nationella lagstiftningen att vem som helst kan klaga över en myndighets åtgärder enbart på grundval av en ospecificerad misstanke om lagstridighet, har det varit möjligt att utfärda bestämmelser som begränsar underrättelseskyldigheten.

Skyddspolisens skyldighet att underrätta den som är föremål för underrättelseinhämtning som avser datatrafik om detta är relativt begränsad enligt de bestämmelser som föreslås i denna lag. Detta ska kompenseras genom bestämmelser i lagen om övervakning av underrättelseverksamheten (/) om att var och en ska ha rätt att lämna en begäran om undersökning som gäller underrättelseinhämtning som avser datatrafik till underrättelseombudsmannen.

En begränsning av underrättelseskyldigheten är motiverad i och med att underrättelseinhämtning som avser datatrafik i olika skeden i olika hög grad kan ingripa i skyddet för hemligheten i fråga om förtroliga meddelanden för olika personer. Om ingripandet har varit lindrigt eller tillfälligt eller om uppgifterna om det har utplånats och inte längre innehas av underrättelse-

myndigheten, kan det inte anses finnas skäl till att informera om saken. Dessutom bör det observeras att Europadomstolens avgörandepraxis förutsätter att man underrättar uttryckligen den person som har varit föremål för informationsinhämtningen. En person som tillfälligt berörs av underrättelseinhämtning som avser datatrafik och vars uppgifter utplånas genast då det har konstaterats att hen är en utomstående räknas inte som föremål för underrättelseinhämtning. Uppdelningen i föremål för underrättelseinhämtning och utomstående används också i bestämmelserna om underrättelse om användning av metoder för inhämtande av information ur telenät. När det gäller teleavlyssning och teleövervakning krävs det att enbart den person underrättas som har berörts av en informationsinhämtningsmetod som använts i syfte att förhindra, avslöja eller utreda personens brott. Det kanske till och med stora antal utomstående som den person som är föremål för informationsinhämtningen under tiden för teleavlyssning eller teleövervakning har kommunicerat med och vars kommunikationshemlighet informationsinhämtningsmetoden alltså också har ingripit i underrättas inte om informationsinhämtningen. På motsvarande sätt underrättas inte personer som av en slump och tillfälligt har berörts av till exempel en täckoperation eller systematisk observation om att informationsinhämtningsmetoden har använts. När det gäller bestämmelserna om underrättelse om underrättelseinhämtning som avser datatrafik är det inte motiverat att i högre grad avvika från de bestämmelser som gäller underrättelse om andra informationsinhämtningsmetoder eller underrättelseinhämtningsmetoder.

Enligt 20 § i lagförslaget ska en person som befinner sig i Finland underrättas om underrättelseinhämtning som avser datatrafik om innehållet i ett förtroligt meddelande som hen har sänt eller tagit emot eller information som hen har lagrat har klarlagts manuellt. Skyldighet att underrätta föreligger inte om man genom underrättelseinhämtning som avser datatrafik enbart har undersökt andra uppgifter om kommunikationen än dess innehåll, eller om meddelandets innehåll har undersökts automatiskt. Syftet med automatisk undersökning av innehållet i ett meddelande är att minska mängden information som blir föremål för manuell behandling. Om ett meddelande utplånas efter en sådan här åtgärd som gjorts i syfte att gallra ut information utan att innehållet har blivit känt av någon tjänsteman hos skyddspolisen, kan en underrättelse inte anses vara motiverad. Det ska inte heller finnas någon skyldighet att underrätta en person som befinner sig utomlands om underrättelseinhämtning som avser datatrafik. Eftersom skyldigheten att underrätta endast ska gälla personer vars förtroliga meddelanden har undersökts vad gäller innehållet omfattar skyldigheten inte heller parterna i främmande staters myndighetskommunikation i och med att kommunikationen inte åtnjuter skydd för hemligheten i fråga om förtroliga meddelanden. Med stöd av en särskild bestämmelse ska underrättelseskyldigheten inte heller gälla personer vars förtroliga meddelanden har undersökts manuellt vad gäller innehållet, om uppgifterna om kommunikationen utan dröjsmål har utplånats i enlighet med de skyldigheter att utplåna information som föreskrivs i lagen. Det är inte motiverat med en underrättelse eftersom de uppgifter som gäller den person som annars skulle ha underrättats har utplånats och innehas inte längre av underrättelsemyndigheten på annat sätt än som en loggantecknin om utplåningen.

Då skyldighet att underrätta om underrättelseinhämtning som avser datatrafik gäller ska bestämmelserna om underrättelse om teleavlyssning i polislagens 5 a kap. tillämpas. Lösningen kan motiveras med att underrättelseinhämtning som avser datatrafik där innehållet i ett förtroligt meddelande har undersökts manuellt är jämförbar med teleavlyssning vad gäller omfattningen av ingripandet i de grundläggande rättigheterna. Av det av bestämmelsen om underrättelse om teleavlyssning ska tillämpas följer att den som har varit föremål för informationsinhämtning utan dröjsmål ska underrättas om saken efter det att syftet med informationsinhämtningen har uppnåtts. Med stöd av ett domstolsbeslut kan underrättelsen emellertid skjutas upp eller helt få utebli, om en uppskjutning är motiverad eller en utebliven underrättelse är nödvändig för att skydda de intressen som anges särskilt och på ett uttömmande sätt i lagen. De

bestämmelser som möjliggör uppskjutning eller utebliven underrättelse på grund av specifika skäl överensstämmer med Europadomstolens avgörandepraxis.

Såsom konstaterat har var och en rätt att anföra klagomål över underrättelseinhämtning som avser datatrafik hos underrättelseombudsmannen oavsett om man har haft rätt att bli underrättad eller inte. Underrättelseombudsmannen ska också övervaka att skyddspolisen tillämpar bestämmelserna om underrättelse på rätt sätt.

Utlämnande av information för brottsbekämpning

Bestämmelserna om utlämnande av information för brottsbekämpning överensstämmer med det som föreslås i 5 a kap. 44 § i polislagen.

4 Propositionens konsekvenser

4.1 Ekonomiska konsekvenser

Förslaget kommer att ha konsekvenser för statsbudgeten. En del av konsekvenserna är bestående, en del är av engångsnatur och beror närmast på investeringar. En del av statens utgifter kommer att orsakas direkt av de ändringar i lagstiftningen som nu föreslås, en del av att det blir ändamålsenligt att öka verksamhetens omfattning. Tidpunkten för utgifterna kräver ännu tilläggsutredningar, bland annat beroende på hur det lagstiftningsprojekt som gäller en revidering av grundlagen framskrider. Utredningen av de ekonomiska konsekvenserna fortsätter. De kostnadseffekter som nämns senare är uppskattningar. I samband med planen för de offentliga finanserna och i samband med beredningen av budgeten och tilläggsbudgeten avgörs dimensioneringen av och tidtabellen för de anslag som till följd av reformen eventuellt krävs under olika moment.

De ekonomiska konsekvenserna av propositionen gäller inom inrikesministeriets förvaltningsområde i synnerhet skyddspolisen, men även polisen i övrigt samt inrikesministeriet, inom justitieministeriets förvaltningsområde domstolar, åklagare och Brottspåföljdsmyndigheten och inom näringslivet teleföretagen. Närmare konsekvensbedömningar presenteras i avsnitten 4.1.1–4.1.4. De ekonomiska konsekvenserna beror främst på behovet av att öka personalen, men även på investeringar av engångsnatur och årliga kostnader för den operativa verksamheten, utbildning och förvaltningen av informationssystem.

Vid bedömningen av de ekonomiska konsekvenserna har man utgått från att lagstiftningen om civil underrättelseinhämtning ska träda i kraft vid ingången av 2019. De uppskattade ekonomiska konsekvenserna konkretiseras det år då lagen träder i kraft, med undantag för vissa utgifter för skyddspolisen som realiseras i förskott redan året före ikraftträdandet. Om lagens ikraftträdande tidigareläggs eller försenas jämfört med den planerade tidpunkten, tidigareläggs eller försenas de ekonomiska konsekvenserna på motsvarande sätt.

Skyddspolisen

Merparten av de ekonomiska konsekvenser som de föreslagna ändringarna medför kommer att gälla skyddspolisen. Den nya lagstiftningen innebär att skyddspolisens uppgifter kommer att öka betydligt i och med att uppgiftsfältet utvidgas och befogenheterna ökar. Eftersom det är fråga om ett större uppgiftsfält än nu och helt nya befogenheter är det inte möjligt att omfördela skyddspolisens nuvarande ekonomiska resurser eller personalresurser på de nya uppgifterna. På så sätt kommer man i samband med planen för de offentliga finanserna och i budgetprocesserna att behöva fatta beslut om alla behov av tilläggsresurser som presenterats här.

Skyddspolisens nuvarande uppdrag är att bekämpa brottslighet. I praktiken ansvarar myndigheten för förhindrande, avslöjande och utredning av sådana landsförräderibrott och högförräderibrott som avses i 12 och 13 kap. i strafflagen samt för förhindrande och avslöjande av sådana terroristbrott som avses i 34 a kap. i strafflagen. Utredningen av terroristbrott hör redan nu i regel till centralkriminalpolisen.

I denna proposition föreslås det att skyddet av den nationella säkerheten ska höra till skyddspolisens uppgifter. Då lagstiftningen träder i kraft förändras skyddspolisens ställning till en kombinerad säkerhetstjänst inom landet och underrättelsetjänst som avser utländska förhållanden, som ska ha till uppgift att inhämta information om hot mot den nationella säkerheten oberoende av om hoten utgör brott eller inte. Grunderna för informationsinhämtning och verksamhetens dimensioner i fråga om tid och område förändras och utvidgas jämfört med nu.

I anslutning till den lagstiftningshelhet som gäller civil underrättelseinhämtning föreslås det att skyddspolisen inte längre ska ha de uppgifter i fråga om förundersökning som för närvarande hör till myndigheten. Skyddspolisen har använt mycket lite av sina personalresurser och sin finansiering till dessa uppgifter under de senaste åren. På så sätt har förslaget i detta avseende inga konsekvenser för personalen och man behöver inte omfördela de nuvarande resurserna.

Skyddspolisens uppgift att förhindra och avslöja brott som äventyrar statens säkerhet förblir oförändrad. Av det att de nya uppgifterna och befogenheterna i anslutning till informationsinhämtning som avser både inhemska och utländska förhållanden riktas till skyddspolisen och att de nuvarande uppgifterna och befogenheterna samtidigt i hög utsträckning blir kvar hos skyddspolisen följer att myndighetens uppgiftsfält och dess skyldigheter blir exceptionellt omfattande även i internationell jämförelse.

Då skyddspolisens uppgiftsfält utvidgas och dess befogenheter ökar beräknas volymen av myndighetens informationsinhämtning växa i proportion med resurserna för informationsinhämtningen. Verkställandet av den nya lagstiftningen kommer att ställa allt högre kvalitetsmässiga, utbildningsmässiga, juridiska och strukturella krav på verksamheten hos myndighetens alla enheter. Den ökade volymen av informationsinhämtning och uppfyllandet av de ovan nämnda kraven så att man kan nå de mål som ställts i fråga om resultatet av lagstiftningen om civil underrättelseinhämtning förutsätter att det görs en ny bedömning av basresurserna för skyddspolisens verksamhet samt investeringar av engångsnatur i IKT. För att de operativa resurserna och beredskapen ska stärkas krävs det att också de funktioner som stöder dem, såsom personal- och ekonomiförvaltningen, stärks.

Ett tillräckligt effektivt utnyttjande av de nya befogenheterna för underrättelseinhämtning och de samhälleliga verkningar som kan uppnås via det när det gäller utrikes- och säkerhetspolitiskt beslutsfattande, säkerhetslägesbilder i rätt tid till myndigheterna och skyddet av de nationalekonomiska intressena kräver att resurser sätts in vid rätt tidpunkt. Resursfördelning, utbildning och verksamhetsplanering bör därför inledas tillräckligt tidigt redan innan lagstiftningen har trätt i kraft.

Volymen av civil underrättelseinhämtning står i proportion till de ekonomiska resurser som anvisats. De ökade anslag som följer grundar sig på att skyddspolisen tillräckligt effektivt och framgångsrikt ska kunna utföra det nya uppdrag som ska föreskrivas för den. Uppskattningen är att myndighetens behov av personalresurser kommer att fördela sig så att cirka 30 procent av de nya tjänster som ska inrättas kommer att vara polistjänster och 70 procent civila tjänster.

Vid bedömningen av de ekonomiska konsekvenserna har man i detta skede utgått från att lagstiftningen om civil underrättelseinhämtning ska träda i kraft vid ingången av 2019. Om tid-

punkten för när något finansieringsbehov realiseras till exempel sägs vara år 2018, innebär detta att det finns ett finansieringsbehov i förskott redan året innan lagen träder i kraft. Om lagens ikraftträdande tidigareläggs eller försenas jämfört med den planerade tidpunkten, tidigareläggs eller försenas de finansieringsbehov som uppstår i förskott på motsvarande sätt. Kostnadsverkningarna av lagstiftningen om civil underrättelseinhämtning specificeras enligt år senare i detta avsnitt.

Det projekt för att höja skyddspolisens prestationsförmåga som pågår hos skyddspolisen täcker inte in de behov som lagen om civil underrättelseinhämtning och lagen om underrättelseinhämtning som avser datatrafik medför.

Utbildning samt personal- och ekonomiförvaltning. När det gäller hemlig informationsinhämtning kan skyddspolisen i fortsättningen inte stödja sig enbart på de utbildningar som planeras och ordnas av Polisyrkeshögskolan och centralkriminalpolisen eftersom grunderna för när befogenheterna inom civil underrättelseinhämtning får användas, taktiska aspekter i anslutning till användningen, helt nya befogenheter och den personkrets som metoderna får riktas in på skiljer sig från de traditionella metoderna för brottsbekämpning. Dessutom är avsikten att metoderna ska användas i en ny verksamhetsmiljö, det vill säga utomlands. Utbildningsstrukturerna för de nya befogenheterna i fråga om civil underrättelseinhämtning måste alltså skapas och etableras inom myndigheten själv. Avsikten är att det ska inrättas en utbildningsenhet inom skyddspolisen, som ska svara för specialutbildning och fortbildning av myndighetens personal samt sådan specialutbildning av befälet som lagen om civil underrättelseinhämtning kräver. Enheten ska också delta i utbildningssamarbete med myndigheten för militär underrättelseinhämtning, domstolarna och laglighetsövervakningen. I detta skede uppskattar skyddspolisen att dess utbildningsfunktion i den inledande fasen kommer att omfatta 6 årsverken, av vilka 2 är tidsbundna, och under driftsfasen 4 permanenta årsverken. En del av den taktiska utbildningen ska köpas in av sådana internationella samarbetsparter som har lång erfarenhet av att använda befogenheter för underrättelseinhämtning. Den ökning av organisationens personal som ändringarna i lagstiftningen kommer att leda till förutsätter också en permanent förstärkning av resurserna i anslutning till personalförvaltningen och myndighetens ekonomiförvaltning och allmänna förvaltning.

Laglighetsövervakningen och det juridiska stödet. Skyddspolisen har för närvarande ingen funktion för intern laglighetsövervakning på heltid, utan den interna laglighetsövervakningen sköts lika som hos polisen i övrigt som bisyssla och i huvudsak i form av periodiska inspektioner.

I och med de nya befogenheterna för underrättelseinhämtning ökar betydelsen av myndighetens interna laglighetsövervakning. Den interna laglighetsövervakningen behöver ordnas så att den sker mera i realtid, blir effektivare och mera heltäckande, och detta kräver att den separeras till en egen funktion, vilket kräver tilläggsresurser (4 årsverken). Samtidigt behöver förhållandet mellan den interna laglighetsövervakningen och de externa organen för laglighetsövervakning fastställas, framför allt när det gäller den tillsynsmyndighet som föreslås i den proposition från justitieministeriet som ansluter sig till denna proposition. Laglighetsövervakningen ska bedriva ett nära samarbete med utbildningsenheten för att sprida rätt tillämpningspraxis till de tjänstemän som använder befogenheterna för underrättelseinhämtning. Ordnandet av den interna laglighetsövervakningen förutsätter delvis finansiering redan innan lagen har trätt i kraft, så att 3 årsverken av de totala personalresurserna som skyddspolisen har uppskattats behöva för funktionen kan tas i bruk året före lagens ikraftträdande. Detta gör det möjligt att fullt ut börja använda metoderna för civil underrättelseinhämtning med rätt tillämpningspraxis och tillräcklig utbildning genast då lagen träder i kraft.

Dessutom ska det inrättas två nya tjänster för jurister med operativ roll vid de operativa enheterna, som ska stödja den operativa informationsinhämtningen när det gäller de nya befogenheterna för underrättelseinhämtning inom landet och underrättelseinhämtning som avser utländska förhållanden samt datatrafik. Dessa tjänster omfattar 4 årsverken av det totala resursbehovet för den interna laglighetsövervakningen. Genom den ovan beskrivna uppdelningen säkerställs det att laglighetsövervakningen och det operativa beslutsfattandet även i fortsättningen hålls separat.

Metodutveckling, analys och operativ informationsinhämtning. I och med lagstiftningen om civil underrättelseinhämtning ökar skyddspolisens uppgifter och utvidgas myndighetens uppgiftsfält. Informationsinhämtning ska framöver grunda sig på skyddet av den nationella säkerheten och inte enbart på förhindrande och avslöjande av brott. Ett effektivt utnyttjande av de nya befogenheterna kräver att den operativa informationsinhämtningen stärks både i form av personalresurser och utrustning och metodutveckling. Med en ökad mängd rådata som myndigheten inhämtat till följd av nödvändiga insatser måste informationens användbarhet säkerställas genom satsningar på den tekniska och operativa analysen av den information som flyter in samt på förbehandlingen av informationen, den fortsatta utredningen av hot och bevakningen av de personer som är i fokus. Effektivare informationsinhämtning och utnyttjande av den information som inhämtats i syfte att skydda Finlands nationella säkerhet kräver också att skyddspolisen utvidgar sitt samarbetsnätverk genom att skapa nya partnerskap med både inhemska och utländska myndighetsaktörer samt andra aktörer. Till följd av detta kommer omfattningen av det operativa samarbetet att öka märkbart.

De personalresurser som behövs för att stärka den operativa verksamheten och samarbetsstrukturerna har uppskattats till 48 årsverken. Det blir fråga om att inrätta nya stadigvarande tjänster. För att befogenheterna för underrättelseinhämtning ska kunna användas effektivt och fullt ut krävs det att den taktiska och tekniska metodutvecklingen inleds i god tid innan lagen träder i kraft och att den operativa personalen är tillräckligt utbildad i att använda sig av befogenheterna före ikraftträdandet. Därför behöver nya tjänster inrättas och utrustning införskaffas delvis redan före lagens ikraftträdande.

Rapportering till statsledningen, myndigheter och andra intressentgrupper. Mängden information som inhämtats av skyddspolisen beräknas öka med de utvidgade grunderna för informationsinhämtning och de nya metoderna för underrättelseinhämtning och ökade resurserna. Ett av de viktigaste målen med lagstiftningen om civil underrättelseinhämtning är att öka och förbättra den information som den högsta statsledningen får in om förändringar i och utvecklingen av Finlands säkerhetsmiljö så att informationen kan stödja ett utrikes- och säkerhetspolitiskt beslutsfattande som sker i rätt tid och på basis av tillräckliga fakta. För att detta ska lyckas krävs det att de underrättelseuppgifter som skyddspolisen inhämtat är analyserade på ett mångsidigt och grundligt sätt när de överlämnas till statsledningen och myndigheterna, så att skyddspolisen på ett optimalt sätt kan stödja deras verksamhet. Då lagstiftningen revideras ökar också förväntningarna på att analyserade underrättelseuppgifter ska produceras även för aktörerna inom den privata sektorn för tryggandet av viktiga ekonomiska samhällsintressen. Det är nödvändigt att det allokeras uppskattningsvis 8 årsverken i resurser för den strategiska analysen och samkörningen av de underrättelseuppgifter som inhämtats med hjälp av de nya befogenheterna såväl som för rapporteringen till de behöriga myndigheterna.

Underrättelseinhämtning som avser datatrafik. På det sätt som framgår av propositionen ska försvarsmaktens underrättelsetjänst fungera som teknisk genomförare när det gäller sådan underrättelseinhämtning som avser datatrafik som sker inom civil underrättelseinhämtning. Skyddspolisen ska ansvara för analysen av den information som förmedlats till den samt för andra fortsatta åtgärder. Av denna lösning följer att kostnaderna för det tekniska genomförandet av underrättelseinhämtning som avser datatrafik i första hand kommer att beröra försvars-

maktens underrättelsetjänst. Bedömningen av de ekonomiska konsekvenserna ingår till denna del i den proposition som gäller lagstiftningen om militär underrättelseinhämtning som ansluter sig till denna proposition. Kostnaderna för sådan underrättelseinhämtning som avser datatrafik som sker inom civil underrättelseinhämtning behandlas i den nedanstående tabellen, men bara i den mån de gäller skyddspolisen. Kostnadsverkningarna för de metoder för underrättelseinhämtning ur telenät som används inom såväl den civila underrättelseinhämtningen som den militära underrättelseinhämtningen ingår i bedömningen av de ekonomiska konsekvenserna för skyddspolisen. Eventuella fördelningar av kostnaderna mellan olika myndigheter granskas ännu särskilt.

Underrättelseinhämtning som avser utländska förhållanden. Befogenheterna för underrättelseinhämtning som avser utländska förhållanden förutsätter att det inrättas en helt ny funktion. Detta kommer att innebära specialutbildad personal, skyddsstrukturer och -processer för informationsinhämtningen och personalen, operativ svarstid dygnet runt enligt behov och internationella samarbetsstrukturer. För att underrättelseinhämtning som avser utländska förhållanden ska kunna genomföras krävs det också att det upprätthålls en stödfunktion i anslutning därtill (bland annat ekonomitjänster och stöd för administrativa skyddsstrukturer och täckmantlar). Stödverksamhet dygnet runt inbegriper också en mera omfattande och stärkt personalsäkerhetsverksamhet, såsom bevakning dygnet runt samt tillhandahållande av ämbetsverkstjänster och fastighetstjänster på det sätt som den operativa verksamheten kräver.

Kostnader för lokaler. De resursökningar som ansluter sig till den nya lagstiftningen om civil underrättelseinhämtning kommer att innebära en personalökning hos myndigheten, vilket i sin tur innebär en ökning av myndighetens lokalkostnader. Skyddspolisen har i detta skede uppskattat att varje nytt årsverke gör att de årliga kostnaderna för lokaler ökar med 7 500 euro.

Parallellt med detta lagstiftningsprojekt pågår ett projekt som gäller skyddspolisens lokaler, där man kartlägger alternativ för hur frågan om lokalerna ska ordnas då hyresavtalet för myndighetens nuvarande lokaler löper ut vid årsskiftet 2019–2020. De kostnader som uppstår på grund av eventuella omarrangemang av lokalerna har inte beaktats i propositionen och de kostnader som lagstiftningen om underrättelseinhämtning medför har tills vidare inte heller beaktats i lokalprojektet.

Sammanfattning av propositionens ekonomiska konsekvenser för skyddspolisen

Sammanfattning av lagförslagets ekonomiska konsekvenser för skyddspolisen	**Tilläggsbudg försl 2018**	**Plan 2019** ***(lagen föreslås träda i kraft)***	**Plan 2020**	**Plan 2021->**
Skyddspolisens omkostnader 26.10.02				
Investeringar av engångsnatur	**9 700 000**	**-**	**-**	**-**
- kostnader för ändring av informationssystem	*700 000*			
- investeringar som gäller underrättelseinhämtning som avser datatrafik	*9 000 000*			
Personalkostnader (årsverken)	**1 911 000 (27 årsverken)**	**6 764 000 (94 årsverken)**	**6 764 000 (94 årsverken)**	**6 614 000 (92 årsverken)**
Övriga årliga kostnader, totalt	**895 000**	**4 405 000**	**4 405 000**	**4 390 000**
- lokal-, säkerhets-, bevaknings- och fastighetstjänster	*195 000*	*1 105 000*	*1 105 000*	*1 090 000*
- fordonsanskaffningar	*-*	*200 000*	*200 000*	*200 000*
- operativa utvecklingskostnader	*400 000*	*1 500 000*	*1 500 000*	*1 500 000*
- linje-, drifts- och licenskostnader, informationssystemens livscykelkostnader samt ersättningar till operatörer	*-*	*1 300 000*	*1 300 000*	*1 300 000*

- extern utbildning	*300 000*	*300 000*	*300 000*	*300 000*
Skyddspolisen, totalt	**12 506 000**	**11 169 000**	**11 169 000**	**11 004 000**

Inrikesministeriet

Skyddspolisens interna övervakning håller god nivå, enligt de observationer som gjorts vid riksdagens justitieombudsmans laglighetsövervakning. Vid ingången av 2016 övergick Skyddspolisen till att vara en enhet under inrikesministeriet och omfattas alltså inte längre av Polisstyrelsens laglighetsövervakning. Inrikesministeriet har enligt justitieombudsmannen mycket små personalresurser, och personalen har också många andra uppgifter. Det bör enligt justitieombudsmannen säkerställas att nivån på kontrollen av skyddspolisen inte sjunker (Riksdagens justitieombudsmans berättelse år 2015, s. 186).

Lagstiftningspaketet om civil underrättelseverksamhet skulle öka skyddspolisens befogenheter att inhämta information samt personalresurserna på ett sätt som kräver att dess interna laglighetsövervakning stärks genom en övervakning som i högre grad sker i realtid. Den utökade verksamheten och övervakningen förutsätter att också inrikesministeriet får nya administrativa och juridiska uppgifter i anknytning till skyddspolisen. Inrikesministeriet har uppskattat att personalbehovet i samband med att ministeriets övervakningsmekanism stärks är minst två årsverken, vilket betyder en kostnad på cirka 175 000 euro.

Att bygga upp förmågan till civil underrättelseverksamhet kommer enligt avsnittet om skyddspolisen ovan att öka skyddspolisens resurser med 92 årsverken. Med tanke på behovet av styrning i anknytning till den civila underrättelseverksamheten och befogenheterna att inhämta underrättelser samt de personalresurser verksamheten kräver, uppskattas det att inrikesministeriets styrning kommer att få ökad betydelse. För att inrikesministeriet ska kunna utföra de uppgifter som åläggs den i de nämnda bestämmelserna, kräver stärkandet av inrikesministeriets styrmekanism att personalresursen ökas med åtminstone två årsverken, dvs. uppskattningsvis 175 000 euro.

Inrikesministeriet tillsatte genom ett beslut (SMDno-2016-1478) den 12 oktober 2016 ett projekt med uppgift att bereda förslag till hur styrningen av den civila underrättelseinhämtningen och skyddspolisen kunde utvecklas inom inrikesministeriets förvaltningsområde. I projektets slutrapport och i denna propositions avsnitt om de ekonomiska konsekvenserna ges närmare uppskattningar av hur mycket styrningen och övervakningen av skyddspolisen kommer att öka arbetsmängden vid inrikesministeriet utöver det uppskattade minimikrav som nämns ovan.

Sammandrag över propositionens ekonomiska konsekvenser för inrikesministeriet	**Tilläggsbudg försl 2018**	**Plan 2019** ***(föreslaget ikraftträdande)***	**Plan 2020**	**Plan 2021 ->**
Inrikesministeriets omkostnader 26.01.01				
Personalkostnader (årsverken)		**350 000 (4 årsv.)**	**350 000 (4 årsv.)**	**350 000 (4 årsv.)**

Övrig polisförvaltning

Det ligger i samhällets helhetsintresse att utreda och i synnerhet förebygga de allra allvarligaste brotten. Det finns därför anledning att i bred omfattning tillåta anmälan av sådana brott. Utlämnande av sådan information är också motiverat av rättviseskäl och med tanke på offret. Regeringen föreslår att det i 5 a kap. 43 § i polislagen och i 17 § i lagen om civil underrättelseinhämtning avseende datatrafik föreskrivs om skyddspolisens rätt och skyldighet att till andra polismyndigheter anmäla brott som framkommer medan en metod för underrättelseinhämtning används. Skyddspolisen ska enligt de nämnda bestämmelserna ha skyldighet att till behörig

myndighet anmäla, om det medan en metod för underrättelseinhämtning används framkommer ett brott som avses i 15 kap. 10 § i strafflagen och som redan begåtts eller ännu kan förhindras. I fråga om ett redan begånget brott som framkommer vid underrättelseinhämtningen ska det i lagen föreskrivas om möjlighet att av nödvändiga skäl skjuta upp anmälan. Vidare ska skyddspolisen få rätt att till behörig myndighet anmäla, om det medan en metod för underrättelseinhämtning används framkommer ett lindrigare brott för vilket sanktionshotet överskrider en viss tidsgräns och som redan begåtts eller ännu kan förhindras. I fråga om redan begångna brott föreslås det lägsta sanktionshotet vara tre års fängelse och för brott som ännu kan förhindras två års fängelse.

Anmälningsskyldigheten och anmälningsrätten ska gälla brott om vilka skyddspolisen får kännedom i samband med att en metod för underrättelseinhämtning används. Metoderna för underrättelseinhämtning föreslås, med undantag av platsspecifik underrättelseinhämtning och underrättelseinhämtning som avser datatrafik, motsvara de hemliga metoder för inhämtande av information om vilka det i nuläget föreskrivs i 5 kap. i polislagen och som skyddspolisen använder för att förhindra och avslöja brott. Ökningen av antalet metoder för underrättelseinhämtning är således tämligen måttlig.

I förslagen till 5 a kap. 3 § i polislagen och 3 § i lagen om civil underrättelseinhämtning avseende datatrafik föreskrivs om föremålen för den civila underrättelseinhämtningen. De hot som motiverar användning av dessa metoder för underrättelseinhämtning utvidgar skyddspolisens befogenheter att inhämta information i huvudsak på två sätt. För det första får information inhämtas om fenomen som allvarligt hotar den nationella säkerheten men inte är brott och inte heller kan antas utvecklas till brott. För det andra kan information inhämtas tidigare än i nuläget, eftersom det skulle bli möjligt att använda metoder för underrättelseinhämtning redan innan den gärning som är föremål för underrättelseinhämtningen har konkretiserats som ett brott som kan förhindras, det vill säga innan det finns en konkret och specificerad misstanke om brott.

Arten av de utvidgningar som nämndes ovan påverkar hur många sådana brott som avses i 15 kap. 10 § i strafflagen och som redan begåtts eller ännu kan förhindras man kan anta att kommer att anmälas till andra polismyndigheter varje år. Till den del användningen av metoder för underrättelseinhämtning riktar sig till ett fenomen som inte ens kan antas utvecklas till ett brott, torde det mycket sällan framkomma brott under användningen av metoden. Till den del det är frågan om tidig underrättelseinhämtning som föregår förhindrande av brott, kan det antas att samma informationsinhämtning i vilket fall kunde utföras senare i form av hemligt inhämtande av information enligt 5 kap. i polislagen.

De brott som skyddspolisen har skyldighet eller rätt att anmäla kan grovt sett indelas i dels brott som är direkt kopplade till det hot som motiverar underrättelseinhämtningen, dels brott som ur underrättelseinhämtningens synvinkel kan jämställas med brott som är kopplade till information som har arten av överskottsinformation. Ett exempel på brott i den förra kategorin är finansiering av terrorism, som kan framkomma när det hot som motiverar underrättelseinhämtningen är terrorism. Ett brott i den senare kategorin är exempel grov stöld som av en händelse framkommer vid inhämtning av underrättelser om spridning av massförstörelsevapen.

Det är sannolikt att brott av den första kategorin kommer fram i viss omfattning vid inhämtningen av underrättelser, medan brott av den senare kategorin sannolikt framkommer mer sällan. Det kan också antas att brott av den första kategorin, särskilt brott av typen förberedelse och stämpling till brott, skulle komma fram uttryckligen när det hot som motiverar användningen av en metod för underrättelseinhämtning är terrorism. Även om antalet terroristbrott som anmäls till förundersökningsmyndigheten sannolikt skulle öka genom ikraftträdandet av

den nya lagstiftningen, måste det också beaktas att lagstiftningen innefattar faktorer som dämpar ökningen. Underrättelseinhämtningen i fråga om terrorism skulle ske på ett tidigare stadium än i nuläget. Åtminstone i vissa fall skulle underrättelseinhämtningen göra det möjligt att vidta tidiga bekämpningsåtgärder som skulle leda till att den verksamhet som är föremål för underrättelseinhämtning överhuvudtaget inte skulle framskrida till ett straffbart förfarande som måste anmälas. Underrättelseinhämtningen kan därför delvis bidra till att minska antalet genomförda brott som föranleder ett straffrättsligt förfarande. Att underrättelseinhämtningen inleds på ett tidigare stadium leder också till att brott upptäcks och anmäls till förundersökningsmyndigheten tidigare än i nuläget. För närvarande överför skyddspolisen i tämligen stor omfattning terroristbrott till förundersökningsmyndigheten, om brotten framkommit under användning av de befogenheter att inhämta information som föreskrivs i 5 kap. i polislagen. Det är uppenbart att vissa av dessa brott skulle upptäckas och anmälas redan i samband med att metoder för underrättelseinhämtning används. Det är då inte frågan om att antalet anmälningar ökar, utan om att de görs tidigare.

När det hot som motiverar underrättelseinhämtningen utgörs av en främmande stats underrättelseverksamhet, kan man anta att det kan komma fram landsförräderibrott enligt 12 kap. i strafflagen. När man prövar om dessa brott ska gå vidare till brottsutredning måste det beaktas att de av exempelvis skäl som anknyter till diplomatisk immunitet ofta inte kan behandlas i en straffprocess. Sådana brott leder snarare till diplomatiska än straffrättsliga åtgärder.

Det har tidigare konstaterats att de metoder för underrättelseinhämtning som enligt propositionen ska tas in i 5 a kap. i polislagen huvudsakligen är de samma som i nuläget utgör hemliga metoder för inhämtande av information enligt 5 kap. i polislagen. Den viktigaste helt nya metoden för underrättelseinhämtning är underrättelseinhämtning som avser datatrafik, om vilket det enligt propositionen ska föreskrivas i en separat lag. Den information som fås genom underrättelseinhämtning som avser datatrafik kan bedömas vara av sådan art att den som sådan sällan leder till att brott upptäcks och anmäls. I betänkandet från den av försvarsministeriet tillsatta arbetsgruppen för en informationsanskaffningslag konstateras det att den information som fås genom underrättelseinhämtning som avser datatrafik i huvudsak utgörs av annan information som anknyter till kommunikationen än information som beskriver innehållet i kommunikationen. Det beror bland annat på att kommunikationen i ökande grad krypteras. Styr- och förmedlingsuppgifterna för kommunikation är av ytterst stor nytta för underrättelseverksamheten, men de ger i regel inte underlag för slutsatsen att något visst brott har begåtts, vilket skulle utlösa skyldigheten eller rätten att anmäla brottet till förundersökningsmyndigheten.

Utifrån de ovan nämnda omständigheterna kan man göra den riktgivande bedömningen att det på grundval av anmälningar som görs till förundersökningsmyndigheten inom ramen för de så kallade brandväggsbestämmelserna (5a kap. 44 §) kan bli aktuellt med två typer av informationsöverlåtelser som ger upphov till en självständig förundersökning. En del av de anmälningar som görs inom ramen för brandväggsbestämmelserna kan dessutom anknyta till redan pågående undersökningar eller vara av den arten att förundersökningsmyndigheten anser att förundersökningströskeln inte överskrids. Vid tillämpningen av brandväggsbestämmelserna bedömer skyddspolisen inte huruvida förundersökningströskeln överskrids, åtminstone inte på det sätt som föreskrivs i förundersökningslagen, utan den bedömningen ska göras av den som tar emot anmälan. Förundersökningsmyndigheten kan göra den bedömningen att den överlåtna informationen enbart kan användas i samband med inhämtning av kriminalunderrättelser. Också denna typ av information ger upphov till åtgärder som har konsekvenser för antalet behövliga årsverken.

Utifrån det som sagts ovan kan man uppskatta att de anmälningar som görs med stöd av 5 a kap. 44 § i polislagen leder till att den övriga polisförvaltningen kommer att behöva ytterligare

20 årsverken, vilket skulle ge en årlig kostnad på 1 180 000 euro. Att täcka detta resursbehov genom förflyttningar från polisförvaltningens andra nuvarande uppgifter är inte möjligt. I nuläget är det frågan om en riktgivande bedömning av minimiresursbehovet.

Sammandrag över propositionens ekonomiska konsekvenser för den övriga polisförvaltningen	**Tilläggsbudg försl 2018**	**Plan 2019** ***(föreslaget ikraftträdande)***	**Plan 2020**	**Plan 2021 ->**
Polisens omkostnader 26.10.01				
Personalkostnader (årsverken)		**1 180 000 (20 årsv.)**	**1 180 000 (20 årsv.)**	**1 180 000 (20 årsv.)**
Övriga årliga kostnader		**140 000**	**140 000**	**140 000**
Effekten av en höjning av polisens årsverken på de övriga årliga kostnaderna (7 000 euro/årsverke)		*140 000*	*140 000*	*140 000*
Övrig polisförvaltning sammanlagt		**1 320 000**	**1 320 000**	**1 320 000**

Justitieförvaltningen

Utlämnande av information för brottsbekämpning skulle för polisens del leda till en ökning på 20 årsverken, vilket skulle ge en årlig utgift på 1 180 000 euro. Inom justitieministeriets förvaltningsområde är behovet av tilläggsanslag på grundval av detta och de tillståndsärenden som kommer att behandlas vid Helsingfors tingsrätt 141 600 euro för rättshjälp, 153 400 euro för åklagarväsendet, 473 800 euro för domstolarna och 944 000 euro för verkställighet av straff.

Justitieministeriets uppskattning grundar sig på de olika myndigheternas andel av kostnaderna för brottsbekämpningen. Polisens brottsbekämpnings andel av kostnaderna för straffprocessen är cirka 42 procent. År 2013 uppgick kostnaderna för polisens brottsbekämpning till 345 miljoner euro, åklagarväsendets till 46 miljoner euro, rättshjälpens till 41 miljoner euro, domstolarnas till 107 miljoner euro och verkställigheten av straff till 278 miljoner euro. Det betyder att varje euro som polisen lägger på brottsbekämpning leder till en kostnad på i genomsnitt 1,36 euro för justitieministeriets förvaltningsområde. Av detta står åklagarna för 0,13 euro, rättshjälpen för 0,12 euro, domstolarna för 0,31 euro och verkställighet av straff för 0,80 euro. Siffrorna grundar sig på uppgifter i Rättspolitiska forskningsinstitutets publikation ”Rikollisuustilanne 2013” (Ville Hinkkanen: Rikollisuuden kustannukset, s. 412). Utöver de uppskattningar som grundar sig på denna kalkyl innefattar domstolsväsendets kostnader en uppskattning av kostnaderna för behandling av skyddspolisens tillståndsyrkanden.

I fråga om konsekvenserna för justitieministeriets förvaltningsområde finns det anledning att särskilt framhålla svårigheten att bedöma konsekvenserna i fråga om verkställigheten av straff. Konsekvenserna är också till den delen beroende av antalet och arten av de ärenden som leder till en straffprocess, vilket är svårt att förutsäga. Det är likaså svårt att bedöma vilken typ av och hur långa straff som kommer att dömas ut. Å andra sidan gäller information som lämnas ut för brottsbekämpning allvarliga brott, vilket kan leda till att ett flertal ovillkorliga straff döms ut varje år. Bedömningen av konsekvenserna fortsätter.

Sammandrag över propositionens ekonomiska konsekvenser för justitieförvaltningen	**Tilläggsbudg försl 2018**	**Plan 2019** ***(föreslaget ikraftträdande)***	**Plan 2020**	**Plan 2021 ->**
Justitieministeriets förvaltningsområde 25.				
Omkostnader för övriga domstolar 25.10.03				
Personalkostnader, inkl. tillståndskostnader		**473 800**	**473 800**	**473 800**

Rättshjälpsbyråernas och konsumenttvistenämndens omkostnader 25.10.04				
Personalkostnader		**141 600**	**141 600**	**141 600**
Åklagarväsendets omkostnader 25.30.01				
Personalkostnader		**153 400**	**153 400**	**153 400**
Brottspåföljdsmyndighetens omkostnader 25.40.01				
Personalkostnader		**350 000**	**350 000**	**350 000**

Sammandrag över lagförslagens ekonomiska konsekvenser

Sammandrag över propositionens ekonomiska konsekvenser	**Tilläggsbudg försl 2018**	**Plan 2019** ***(föreslaget ikraftträdande)***	**Plan 2020**	**Plan 2021 ->**
Inrikesministeriets förvaltningsområde 26.				
Skyddspolisens omkostnader 26.10.02				
Investeringar av engångsnatur	**9 700 000**	**-**	**-**	**-**
- varav kostnader för ändring av data-system	*700 000*			
- varav investeringar i underrättelse-inhämtning som avser datatrafik	*9 000 000*			
Personalkostnader (årsverken)	**1 911 000 (27 årsv.)**	**6 764 000 (94 årsv.)**	**6 764 000 (94 årsv.)**	**6 614 000 (92 årsv.)**
Övriga årliga kostnader samman-lagt	**895 000**	**4 405 000**	**4 405 000**	**4 390 000**
- varav lokal-, säkerhets-, bevaknings- och fastighetstjänster	*195 000*	*1 105 000*	*1 105 000*	*1 090 000*
- varav fordonsanskaffningar	*-*	*200 000*	*200 000*	*200 000*
- varav operativa utvecklingskostnader	*400 000*	*1 500 000*	*1 500 000*	*1 500 000*
- varav linje-, underhålls- och licens-kostnader, livscykelkostnader för data-system och ersättningar till operatörer	*-*	*1 300 000*	*1 300 000*	*1 300 000*
- varav extern utbildning	*300 000*	*300 000*	*300 000*	*300 000*
Skyddspolisen sammanlagt	**12 506 000**	**11 169 000**	**11 169 000**	**11 004 000**
Polisens omkostnader 26.10.01				
Personalkostnader (årsverken)		**1 180 000 (20 årsv.)**	**1 180 000 (20 årsv.)**	**1 180 000 (20 årsv.)**
Övriga årliga kostnader		**140 000**	**140 000**	**140 000**
Effekten av en höjning av polisens års-verken på de övriga årliga kostnader-na (7 000 euro/årsverke)		*140 000*	*140 000*	*140 000*
Övrig polisförvaltning sammanlagt		**1 320 000**	**1 320 000**	**1 320 000**
Inrikesministeriets omkostnader 26.01.01				
Personalkostnader (årsverken)		**350 000 (4 årsv.)**	**350 000 (4 årsv.)**	**350 000 (4 årsv.)**
Justitieministeriets förvaltningsområde 25.				
Omkostnader för övriga domstolar 25.10.03				
Personalkostnader, inkl. tillstånds-kostnader		**473 800**	**473 800**	**473 800**
Rättshjälpsbyråernas och konsumenttvistenämndens omkostnader 25.10.04				
Personalkostnader		**141 600**	**141 600**	**141 600**
Åklagarväsendets omkostnader 25.30.01				
Personalkostnader		**153 400**	**153 400**	**153 400**

Brottspåföljdsmyndighetens omkostnader 25.40.01				
Personalkostnader		**350 000**	**350 000**	**350 000**

4.2 Konsekvenser för samhällsekonomin och företagen

Underrättelselagstiftningens konsekvenser för samhällsekonomin, företagen och näringslivet måste bedömas samlat. Vid bedömningen av konsekvenserna av lagstiftningen måste man beakta särskilt konsekvenserna för digitaliseringsutvecklingen i samhället och för företagens verksamhetsbetingelser, eftersom det med tanke på den ekonomiska tillväxten är nödvändigt att effektivt utnyttja de möjligheter IT- och kommunikationstekniken ger att lägga om arbetssätten och höja produktiviteten.

Syftet med lagstiftningen om civil underrättelseinhämtning är att skydda Finlands nationella säkerhet och den därtill hörande samhällsekonomin. Det centrala syftet med lagstiftningen om civil underrättelseinhämtning är att inhämta information om hot mot de intressen som är centrala för Finlands nationella säkerhet och även mot samhällsekonomin samt att avvärja dessa hot. En utveckling av underrättelselagstiftningen kan därför bedömas höja tröskeln för främmande stater att spionera på vårt land eller utöva annan skadlig verksamhet via datanäten. Den ökande förmågan till underrättelseinhämtning minskar likväl inte behovet eller vikten av att samfund och enskilda själva skyddar sig. Deras skyddsåtgärder utgör också i fortsättningen de viktigaste medlen för att avvärja olika hot. En fungerande reglering och de nya kapaciteterna kompletterar dock säkerheten i Finlands digitala miljö och främjar näringslivets möjligheter att skydda sig mot hot från främmande makter. Betydelsefullt i det här avseendet är exempelvis det, att information som erhållits genom användning av metoder för underrättelseinhämtning vid behov kunde överlåtas till företag i syfte att avvärja allvarliga hot eller försvara viktiga ekonomiska intressen.

Det är viktigt för samhällsekonomin och för företagen, som utgör en del av samhällsekonomin, att den rättsliga grund som Finland skapar för underrättelsemyndigheternas verksamhet är klar och tydlig. En tillräckligt exakt och balanserad lagstiftning skapar den förutsägbarhet som företagen behöver för planeringen av sin verksamhet och för investeringsbesluten. I ett läge där regleringen av underrättelseverksamheten och vikten av dataskydd accentueras på den digitala marknaden kan en exakt, rättvis och proportionell reglering utgöra en positiv konkurrensfaktor för Finland på den internationella marknaden. Bland annat därför har strävan varit att utforma lagförslagen så att de motsvarar dessa kriterier.

Det krävs samarbete mellan den offentliga och den privata sektorn för att identifiera och avvärja hot mot samhället och bevara den kritiska infrastrukturen och den ekonomiska livsdugligheten hos samhället. Det betyder ett smidigt informationsutbyte mellan underrättelsemyndigheterna och den privata sektorn. Lagförslagen syftar till att skapa en tillräcklig rättslig grund för att skyddspolisen ska kunna lämna ut information till företagen i syfte att skydda deras viktiga intressen. Information som erhålls genom underrättelseverksamheten ska vid behov kunna lämnas ut till privata samfund i syfte att göra det möjligt att avvärja allvarliga hot eller förhindra betydande ekonomiska förluster. Bestämmelser om detta ingår bland annat i den föreslagna lagen om civil underrättelseinhämtning avseende datatrafik.

Konsekvenser för näringslivets konkurrenskraft och investeringar

Näringslivets arbetar i en global miljö där ekonomin och värdenätverken är internationella. I den globala konkurrensen kan också små faktorer ge stort utslag. Företagen placerar sina funktioner landsvist och optimerar hela sin företagsverksamhet utifrån de egna företagsspecifika konkurrensfördelarna. Placeringsbesluten grundar sig på en helhetsbedömning som utgår

från företagens affärsverksamhet och beaktar olika faktorer som exempelvis marknadsfaktorer, beskattning, energitillgång, teknisk kompetens, finländarnas höga utbildningsnivå, tillförlitlighet och ärlighet, skyldigheter i anknytning till arbetskraften, den utvecklade infrastrukturen och det utvecklade samhället, den samhälleliga och politiska stabiliteten, konsumtionsbeteendet och klimatmedvetenheten, lagstiftningen och dess förutsebarhet, stabilitet och noggranna avgränsning, den administrativa bördan och eventuella juridiska risker.

Den finländska näringsstrukturen har blivit tjänstecentrerad och ekonomin innovationsbaserad. Finland har övergått till kompetens- och teknikintensiva branscher och klustren inom dessa sektorer lockar utländska direkta investeringar. Informations- och kommunikationstekniken har stigit fram som en särskild styrka, och den informationsintensiva industrins ekonomiska betydelse ökar. Konsekvenserna för företagsverksamheten varierar beroende bland annat på företagets bransch och storlek och omfattningen av dess internationella verksamhet.

En exakt, rättvis och proportionell reglering av underrättelseverksamheten stärker Finlands rykte som en förutsebar och tillförlitlig företagsmiljö. Det gäller såväl företag som redan är etablerade i Finland som nya aktörer som kan tänka sig att göra investeringar i Finland.

Under beredningen av lagstiftningen har konsekvenserna för Finlands internationella konkurrenskraft och Finlands dragningskraft som investeringsland bedömts. Staternas överdimensionerade nätövervakning och underrättelseinhämtning som avser datatrafik anses enligt internationella undersökningar ha negativa effekter för medborgarnas förtroende för de digitala tjänsterna och för IKT-branschens möjligheter att få internationella kunder eller göra investeringar i de aktuella länderna. Väsentligt för IKT-företagens konkurrenskraft är att den föreslagna regleringen inte förpliktar företagen att försvaga produkternas eller tjänsternas tillförlitlighet exempelvis genom utlämnande av krypteringsnycklar, installering av bakdörrar, begränsningar av användningen av krypteringsprodukter eller andra skyldigheter som skadar affärsverksamheten.

Med tanke på Finlands rykte bör det noteras att regleringen inte ger underrättelsemyndigheten direkt eller obegränsad tillgång till all datatrafik eller till innehållet i företagens datalager på finländskt territorium. Användningen av befogenheter som rör integritetsskyddet anknyter till domstolarnas tillståndsförfarande och behovet av att utnyttja dessa befogenheter måste kunna motiveras fullt ut och specificeras tillräckligt väl. Ett trovärdigt tillsynssystem och kontrollen av myndigheternas verksamhet är väsentliga faktorer för de internationella IKT-företag som bedömer regleringsmiljön i Finland och förutsättningarna att bedriva affärsverksamhet här. Skyddet för företagshemligheter stöds å sin sida av de lagfästa behandlingsförbuden och skyldigheterna att utplåna information samt skrivningarna angående underrättelsemyndigheternas internationella informationsutbyte.

Med hänsyn till alla i Finland verksamma företag, och i synnerhet de företag som definieras som dataöverförare, har beredningen av lagstiftningen beaktat att de skyldigheter regleringen medför måste vara klara, transparenta och förutsebara. Regleringen av underrättelseinhämtning som avser datatrafik påför inte de företag som betraktas som dataöverförare eller andra företag sådana skyldigheter som hör till en myndighet. Dataöverförarnas skyldighet att biträda definieras tydligt i den föreslagna regleringen.

I samband med det betänkande om en informationsanskaffningslag som föregick lagstiftningsarbetet utreddes eventuella negativa konsekvenser som underrättelseverksamhet riktad mot datatrafiken kan ha på investeringarna i Finland. Det konstaterades att det är svårt att bedöma konsekvenserna, men som jämförelseobjekt utnyttjades Sverige, som tämligen detaljerat och offentligt föreskrivit om underrättelseinhämtning som avser datatrafik. Utredningen upptäckte inte några sådana avvikelser i den allmänna utvecklingen för de utländska investeringarna som

kunde förklaras med hänvisning till Sveriges lagstiftning om underrättelseinhämtning som avser datatrafik. Enligt utredningen har ikraftträdandet av lagen ingen klarlagd betydelse för utvecklingen av de utländska investeringarna i Sverige jämfört med de utländska investeringarna i Finland och Danmark. Sverige har exempelvis klarat sig bättre än Finland enligt indexet Data Center Risk Index. Likaså är Finland också nu då lagberedningen pågår aktuellt som placeringsland för nya datacenterinvesteringar.

I nuläget har myndigheterna endast begränsad förmåga att upptäcka statliga spionprogram eller spionoperationer som allvarligt skadar den nationella säkerheten. Underrättelseinhämtning som avser datatrafik skulle likväl i hög grad komplettera Finlands skydd mot allvarligare datanätshot. Underrättelseinhämtning som avser datatrafik skulle därmed vara till nytta också genom att den skyddar näringslivet mot de allra allvarligaste datanätshoten.

Konsekvenser för FoU-verksamheten och för uppkomsten av ny företagsverksamhet

Ett effektivt och pålitligt underrättelsesystem förutsätter att myndigheterna investerar i den teknik och kompetens som underrättelseverksamheten kräver. Befogenheterna att inhämta underrättelser förutsätter investeringar i teknik och satsningar på säker produktutveckling. Till följd av verksamhetens natur måste investeringarna särskilt beakta säkerheten hos den teknik som anskaffas och de för systemens funktion väsentliga omständigheterna i anslutning till försörjningstryggheten. Likaså måste man beakta möjligheterna att utnyttja avtalsbaserad serviceproduktion, eftersom det är nödvändigt att anskaffa teknisk kompetens och resurser också av den privata sektorn. I dagens läge, när den digitala tekniken utvecklas snabbt, kan det leda till att det uppstår nya arbetstillfällen och ny kompetens i Finland.

4.3 Konsekvenser för myndigheterna

Avsikten är att lagstiftningen om civil underrättelseinhämtning ska förbättra möjligheterna att inhämta information till skydd för den nationella säkerheten och därigenom stärka den högsta statsledningens möjligheter att få information om förändringar i säkerhetsmiljön och hot mot den nationella säkerheten. Vid sidan av skyddspolisen får också andra myndigheter som svarar för den nationella säkerheten och myndigheter som samarbetar med skyddspolisen bättre tillgång till information som de behöver för sina uppgifter. Lagförslagen förändrar dock inte dramatiskt det existerande myndighetssamarbetet eller myndigheternas förfaranden.

Samarbetet mellan skyddspolisen och de militära underrättelsemyndigheterna skulle dock bli tätare, eftersom de får samma befogenheter att inhämta underrättelser och det också på lagnivå föreskrivs om deras samarbete inom underrättelseverksamheten. Samarbetet mellan skyddspolisen och de militära underrättelsemyndigheterna förutsätter utöver ett praktiskt och operativt samarbete även exempelvis gemensam utbildning och harmonisering av operativa förfaranden. Samarbetet antas bli intensivt särskilt inom underrättelseinhämtning som avser datatrafik, eftersom det tekniska utförandet enligt förslaget ska skötas av försvarsmaktens underrättelsetjänst.

Vid justitieministeriet ska det dessutom på det sätt som föreslås i en proposition som anknyter till denna proposition inrättas en ny myndighet med uppgift att övervaka lagligheten i den underrättelseinhämtning som skyddspolisen och de militära underrättelsemyndigheterna utför. Justitieministeriets proposition behandlar närmare vilka konsekvenser övervakningen av underrättelseinhämtningen har för myndigheterna. En arbetsgrupp tillsatt av riksdagens generalsekreterare bereder som bäst ett förslag till ordnande av den parlamentariska tillsynen över underrättelseverksamheten.

De största konsekvenserna för myndigheter kommer förslaget att ha på skyddspolisens uppgifter och förfaranden. Skyddspolisen blir genom förslaget en civil underrättelsemyndighet, det vill säga en myndighet med lagfäst rätt att använda metoder för underrättelseinhämtning för att i Finland och utomlands inhämta information om verksamhet som allvarligt hotar den nationella säkerheten. Den förändrade uppgiftsbilden medför för skyddspolisens del konsekvenser som anknyter till den operativa verksamheten, utbildningen, utvecklingen av system och metoder samt laglighetsövervakningen. Hur detta påverkar personalbehovet och andra resurser bedöms närmare i avsnittet om ekonomiska konsekvenser.

Tillståndsärenden som gäller metoder för underrättelseinhämtning och underrättelseinhämtning som avser datatrafik enligt 5 a kap. i polislagen behandlas vid Helsingfors tingsrätt. Den föreslagna lagstiftningen ökar antalet tillståndsyrkanden hos domstolen. Utöver den växande informationsinhämtningen är det troligt att antalet tillståndsyrkanden ökar till följd av att domstolen får rätt att besluta om helt nya metoder för underrättelseinhämtning (platsspecifik underrättelseinhämtning och underrättelseinhämtning som avser datatrafik

Den föreslagna lagstiftningen innefattar å andra sidan ett flertal faktorer som är ägnade att begränsa ökningen av antalet tillståndsyrkanden. En sådan faktor är att de hot som kan utgöra grund för användning av metoder för underrättelseinhämtning definieras uttömmande och tämligen strikt. Området för de hot som motiverar underrättelseinhämtning är delvis betydligt snävare än skyddspolisens lagfästa verksamhetsområde. Skyddspolisen har bland annat i uppgift att förhindra och avslöja brott som planeras eller begås av inhemska extremiströrelser, men underrättelseinhämtningen syftar inte till att inhämta information om sådana rörelsers verksamhet. En annan faktor som dämpar den relativa ökningen av antalet tillståndsyrkanden är att tillståndens längsta giltighetstid föreslås bli betydligt längre än för de tillstånd som beviljas med stöd av 5 kap. i polislagen. Den längsta giltighetstiden såväl för metoder för underrättelseinhämtning enligt 5 a kap. i polislagen som för underrättelseinhämtning som avser datatrafik föreslås vara sex månader, medan den för hemliga informationsinhämtningsmetoder enligt 5 kap. i polislagen är en månad. Vid en långvarig spaningsoperation kan det därmed på ett år bli aktuellt med endast två tillståndsyrkanden i stället för tolv yrkanden, vilket vore fallet om den längsta giltighetstiden var den samma som i 5 kap. i polislagen. En tredje faktor som dämpar ökningen av antalet tillstånd är det att tillstånd för teleavlyssning och teleövervakning kan sökas inte bara för en enskild teleadress eller teleterminalutrustning utan också med avseende på en person. Om det under tillståndets giltighetstid kommer fram att den person som är föremål för underrättelseinhämtningen använder nya teleadresser eller teleterminalutrustningar, behöver nya domstolstillstånd inte sökas för dem.

Utöver det som sagts ovan bör det noteras att underrättelseinhämtning som i framtiden sker med stöd av 5 a kap. i polislagen i någon mån kan minska behovet av eller åtminstone dämpa ökningen av hemliga informationsinhämtningsmetoder enligt 5 kap. i polislagen. Det är inte frågan om en förskjutning i den meningen att ett yrkande som i nuläget framförs med stöd av 5 kap. i framtiden skulle framföras med stöd av 5 a kap. Snarare är det frågan om att underrättelseinhämtning på ett tidigt stadium och de bekämpningsåtgärder som den möjliggör kan minska risken för att den verksamhet som är föremål för underrättelseinhämtningen överhuvudtaget konkretiseras som ett brott som kan förhindras och därmed skulle kräva användning av de metoder som avses i 5 kap. Också den underrättelseinhämtning som avser utländska förhållanden är ägnad att minska risken för att den verksamhet som är föremål för underrättelseinhämtningen flyttas till Finland och konkretiseras i form av ett brott som kan förhindras. Det är dock svårt att åtskilja konsekvenserna av att det lagstiftas om underrättelseinhämtning och de därav oberoende konsekvenserna av förändringarna i omvärlden.

I förslaget ingår en bestämmelse om övervakning av användningen av metoder för underrättelseinhämtning och ett bemyndigande att genom förordning av statsrådet utfärda närmare be-

stämmelser. Genom förordning ges närmare bestämmelser om skyldigheterna i fråga om registrering, protokollföring, rapportering och övervakning i anknytning till metoderna för underrättelseinhämtning. Till den här delen innebär den föreslagna lagstiftningen ingen nämnvärd förändring jämfört med de gällande förfarandena, eftersom det i fråga om metoder för underrättelseinhämtning föreslås att bestämmelserna ges på förordningsnivå på samma sätt som i fråga om hemliga metoder för inhämtande av information och hemliga tvångsmedel.

4.4 Samhälleliga konsekvenser

Medborgarnas ställning i samhället och det civila samhällets verksamhet

Lagstiftningen om civil underrättelseinhämtning innebär ett ingrepp mot rättsliga intressen som skyddas i grundlagen och genom de internationella människorättsåtagandena, i synnerhet skyddet för privatlivet och hemligheten i fråga om förtroliga meddelanden. Europadomstolen har i sin avgörandepraxis ansett att en reglering som möjliggör intrång i förtrolig kommunikation redan i sig begränsar den rätt som med stöd av artikel 8.2 i Europakonventionen hör till var och en, oberoende av om åtgärder för informationsinhämtning faktiskt vidtagits eller inte (Liberty and others, punkt 56 och Weber and Saravia, punkt 78). Förslaget begränsar således den enskildes rätt till skydd för privatlivet och rätt till hemlighet för förtroliga meddelanden enligt 10 § i grundlagen och artikel 8.2 i Europakonventionen.

De föreslagna bestämmelserna om befogenheter är därför noga avgränsade och exakt utformade, vilket betyder att tillämpningen av bestämmelserna är förutsägbar ur medborgarnas synvinkel. Syftet med regleringen är att skydda den nationella säkerheten, vilket har positiva konsekvenser för den enskilda medborgarens säkerhet. Lagförslagen är utformade med hänsyn till proportionalitetsprincipen, principen om minsta olägenhet och kraven på effektiva rättstrygghetsförfaranden.

Propositionen har inga konsekvenser för medborgarnas möjligheter till delaktighet och medinflytande i samhället, exempelvis i form av verksamhet i politiska partier eller i fackliga eller andra organisationer eller föreningar.

Frågorna i anknytning till de grundläggande fri- och rättigheterna och de mänskliga rättigheterna behandlas närmare i avsnittet om förhållande till grundlagen och lagstiftningsordning.

Brottsbekämpning och säkerhet

Underrättelseinhämtning och brottsbekämpning, särskilt utredning av brott, har olika syften. Syftet med underrättelseinhämtning är inte att den ska leda till straffansvar, utan att stödja den högsta statsledningens beslutsfattande med hjälp av information som inte kan erhållas på något annat sätt. Vidare syftar underrättelseinhämtningen till att göra det möjligt att så tidigt som möjligt upptäcka och avvärja allvarliga hot mot den nationella säkerheten.

Det kan antas att underrättelseverksamheten ger information inte bara om hot utan också om brott som äventyrar den nationella säkerheten, exempelvis terroristbrott. När det under underrättelseinhämtningen framkommer hot mot den nationella säkerheten eller andra allvarliga brott, ska skyddspolisen enligt förslaget anmäla saken till den behöriga myndigheten eller förundersökningsmyndigheten. Skyddspolisen får dessutom enligt vad som särskilt föreskrivs lämna ut information till förundersökningsmyndigheten för förhindrande och avvärjande av brott.

Förslaget kan antas stärka förundersökningsmyndighetens möjligheter att få information åtminstone om de allra allvarligaste brotten. Förslagets konsekvenser för brottsbekämpningen

tar sig dessutom uttryck i att den behöriga myndigheten får bättre möjligheter att förhindra brott. Genom den nya lagstiftningen förbättras möjligheterna att i enskilda fall förhindra att en situation utvecklas från förberedelse till verkställande av ett allvarligt brott.

Konsekvenser för informationssamhället

Lagstiftningen om civil underrättelseinhämtning har såväl direkta som indirekta konsekvenser för informationssamhället. Konsekvenserna följer framför allt av den nya befogenheten ifråga om underrättelseinhämtning som avser datatrafik. Konsekvenserna av de nya befogenheterna i fråga om underrättelseinhämtning som föreslås bli införda i polislagen är mer begränsade, eftersom de till sin digitala natur är samma metoder som det föreskrivs om i 5 kap. i polislagen (teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, teknisk avlyssning).

Hur stora konsekvenserna blir för informationssamhället kan i väsentlig grad påverkas genom lagstiftningstekniska lösningar. Vid valet av lösningar för lagstiftningen har beredningen därför från första början bedömt konsekvenserna av regleringen och tagit hänsyn till den offentliga debatt som lagstiftningsprojektet gett upphov till.

Konsekvenserna för IKT-företagens konkurrenskraft tangerar konsekvenserna för informationssamhället. I fråga om dem behandlas endast de direkta konsekvenserna i det här kapitlet. De indirekta konsekvenserna för företagen behandlas i samband med de samhällsekonomiska konsekvenserna.

Konsekvenserna av lagstiftningen om underrättelseinhämtning som avser datatrafik på tjänsterna i informationssamhället

Underrättelseinhämtning som avser datatrafik bedöms ge konsekvenser för skyddet för sådan förtrolig kommunikation som bedrivs av personer som är utomstående i förhållande till föremålet för underrättelseinhämtningen. Strävan har varit att genom lagstiftningstekniska val begränsa intensiteten i ingreppen så att ingens rätt inskränks mer än nödvändigt.

Underrättelseinhämtning som avser datatrafik ska enligt förslaget utföras genom filtrering av datatrafiken i trafikknutpunkterna. En effektiv underrättelseinhämtning som avser datatrafik förutsätter att filtreringssystemet ser en så stor del som möjligt av den för spaningen väsentliga datatrafiken hos föremålet för underrättelseinhämtningen. Av det följer å andra sidan att också utomstående datatrafik (överskottsinformation) flödar genom filtreringssystemet.

Även om underrättelseinhämtning som avser datatrafik endast tillämpas på datatrafik som överskrider rikets gränser, kan till följd av internets funktionssätt också datatrafik inom landet bli föremål för filtrering. Vid exempelvis belastningstoppar eller funktionsfel kan kommunikation mellan två parter i Finland styras via en router i utlandet. Det är då möjligt att det vid den fortsatta behandlingen av automatiskt separerad datatrafik framgår att datatrafiken var av inhemsk karaktär. Förslaget innefattar därför ett förbud mot underrättelseinhämtning där föremålet för inhämtningen är inhemsk kommunikation. Likaså ingår en skyldighet att utplåna information från inhemsk kommunikation genast när den upptäcks.

Konsekvenser för säkerheten och för skyddet av kritisk informationsinfrastruktur

Underrättelseinhämtning som avser datatrafik bedöms ha positiva konsekvenser för informationssäkerheten och skyddet av kritisk informationsinfrastruktur i Finland.

Det är i regel mest effektivt att skydda informationen och upptäcka avvikelser i informationssäkerheten så nära den information som ska skyddas som möjligt. I 272 § i lagen om tjänster inom elektronisk kommunikation föreskrivs att teleföretag, sammanslutningsabonnenter och leverantörer av mervärdestjänster har rätt att vidta nödvändiga åtgärder enligt 2 mom. för att sörja för informationssäkerheten i syfte att upptäcka, förhindra och utreda störningar som kan inverka menligt på informationssäkerheten i kommunikationsnäten eller tjänster som anslutits till dem samt i informationssystemen och göra störningarna föremål för förundersökning. I en stor del av de fall som kränker informationssäkerheten fungerar de bekämpningsåtgärder som avses i lagen om tjänster inom elektronisk kommunikation bra, eftersom den kvantitativt största delen av avvikelserna i informationssäkerheten uppstår till följd av automatiska attacker, vilket betyder att också bekämpningsåtgärderna effektivt kan automatiseras. Situationen är dock en helt annan när det gäller sådant statligt baserat cyberspionage som inte utgör automatisk massinhämtning utan sker genom noggrant riktade manuella attacker.

Det har visat sig vara osannolikt att cyberspionage upptäcks genom de åtgärder som anges i 272 § i lagen om tjänster inom elektronisk kommunikation. Det problematiska i den rådande situationen har klart erkänts i en färsk forskningspublikation där det konstateras att cyberspionaget utgör en nationell blind punkt. Det har på det stora hela blivit allt mer komplicerat att kontrollera datariskerna. På grund av att underleverantörskedjorna ofta är långa har ett flertal aktörer tillgång till information som är kritisk för en organisation. Även om varje tjänsteleverantör i och för sig sköter det tekniska skyddet med omsorg och även om tjänsteavtalen är skickligt utformade, har de organisationer som har lagt ut sin IT-förvaltning på entreprenad inte längre tekniska möjligheter att själva upptäcka avvikelser i behandlingen av informationen. Å andra sidan kan inte ens en yrkesskicklig tjänsteleverantör identifiera en händelse som en avvikelse, om händelsens betydelse kan förstås enbart genom ingående kännedom om kundorganisationens verksamhet. Helhetsansvaret för skyddet av informationen kvarstår dock hos organisationen själv, vilket inte heller förändras när förmågan att upptäcka informationsrisker som hotar den nationella säkerheten förbättras.

Samtidigt som förutsättningarna att upptäcka avvikelser rentav har försvagats, har informationens betydelse som den mest centrala produktionsfaktorn i informationssamhället ökat. Informationens integritet och konfidentialitet och tillgången till information är numera så väsentliga och skyddsvärda intressen att hela samhället, var och en inom sin sektor, måste bidra till skyddet. Utöver den informationssäkerhetsverksamhet som bedrivs av de organisationer som äger informationen, IKT-tjänsteleverantörerna och de företag som tillhandahåller informationssäkerhetstjänster behövs det effektiva myndigheter med förutsättningar att upptäcka och avvärja hot mot Finland. Cybersäkerhetscentralen vid Kommunikationsverket utför ett värdefullt arbete inom informationssäkerhet och utgör ett stöd för företagen och den offentliga förvaltningen. Det räcker dock inte, utan det behövs dessutom bättre förmåga att identifiera också noggrant riktade statligt baserade cyberhot redan innan de har börjat realiseras. Underrättelseinhämtning som avser datatrafik förbättrar de behöriga myndigheternas förutsättningar att upptäcka såväl cyberkartläggning av kritisk infrastruktur som statligt cyberspionage som av aktörer utomlands riktas mot högteknologisk forskning och produktutveckling i Finland.

Såväl den kritiska informationsinfrastrukturen som den högteknologiska produktutvecklingsinformationen besitts i Finland i huvudsak av privata företag. Därför ger lagen om underrättelseinhämtning avseende datatrafik möjlighet att i syfte att förebygga skada lämna ut information om hot mot informationssäkerheten till såväl kommunikationsverket som företag som utsätts för en främmande stats informationsinhämtning. Det krävs samarbete mellan många aktörer för att upprätthålla informationssäkerheten. Underrättelseinhämtning som avser datatrafik bidrar med ytterligare en komponent i detta samarbete.

Konsekvenser för leverantörer av informationssamhällstjänster

När det gäller leverantörerna av informationssamhällstjänster har de metoder för underrättelseinhämtning som avses i 5 a kap. i polislagen (teleavlyssning, inhämtande av information i stället för teleavlyssning och teleövervakning) konsekvenser åtminstone för teleföretagen, som är skyldiga att biträda myndigheterna och göra de kopplingar i ett telenät som krävs för underrättelseinhämtningen. Teleföretagens arbetsbörda ökar, men det kan förväntas att de förlängda tillståndstiderna dämpar ökningen. Tillstånd för metoder för underrättelseinhämtning via telenätet kan enligt förslaget beviljas för sex månader åt gången. I mer långvariga spaningsoperationer minskar det belastningen på teleföretagens personalresurser jämfört med om tillståndens giltighetstid följer bestämmelserna i 5 kap. Medan teleavlyssning som sker med stöd av ett tillstånd enligt 5 kap. förutsätter att teleföretaget utför kopplingen med en månads mellanrum, tillåter de föreslagna befogenheterna att teleföretaget utför åtgärden med sex månaders mellanrum.

Konsekvenserna av den nya underrättelseinhämtning som avser datatrafik är större för leverantörerna av informationssamhällstjänster är större, eftersom det i nuläget inte finns någon motsvarande reglering. Konsekvenserna gäller enbart så kallade dataöverförare, med vilka avses dem som äger eller innehar den del av ett kommunikationsnät som överskrider Finlands gräns. Det finns i nuläget uppskattningsvis ett tiotal sådana företag. Lagstiftningen om underrättelseinhämtning som avser datatrafik påför skyldigheter vars direkta kostnader, inklusive personalkostnader, likväl ersätts av statens medel.

I de föreslagna bestämmelserna om underrättelseinhämtning som avser datatrafik ingår inga skyldigheter för dataöverförarna eller andra företag att försvaga de kundlöften som är förknippade med programvaruprodukterna eller informationssamhällstjänsterna genom att exempelvis lämna ut krypteringsnycklar, installera bakdörrar eller införa begränsningar i användningen av krypteringsprodukter.

Inriktningen av underrättelseinhämtning på datatrafiken i ett kommunikationsnät

Det är svårt att få en klar bild av mängden data som rör sig i kommunikationsnäten. Mängden data som vid varje tidpunkt överförs i kommunikationsnäten beror bland annat på hur datan överförs i de andra delarna i det globala kommunikationsnätet. I exempelvis internet styrs datatrafiken via de rutter genom vilka datan snabbast når destinationen.

Den mest exakta bilden av datatrafikens volym i en del av kommunikationsnätet vid varje tidpunkt har den som förvaltar den delen av nätet. I praktiken är det ägaren till den delen av kommunikationsnätet eller exempelvis den som hyr en singelfiber. Uppgifter om detta finns dock inte tillgängliga, eftersom de omfattas av företagshemligheten.

Mängden överförda data kan dock uppskattas utifrån den statistik som publiceras av dem som driver knutpunkter (internet exchange, IX) för datatrafik över internet i närområdet. Endast en del av datatrafiken går via de centrala knutpunkterna, men på basis av statistiken kan man uppskatta att den från Finland utgående och till Finland ankommande datamängden uppgår till 1 terabit per sekund, medan mängden data som styrs via Finland uppskattas till 5–10 terabit beroende på situation.

Vid underrättelseinhämtning som avser datatrafik riktas underrättelseinhämtningen till de delar av ett kommunikationsnät som anges i domstoltillståndet, exempelvis till en singelfiber, ett fiberpar eller en våglängd i en optisk kabel som överskrider Finlands gräns. Antalet fiberpar i en optisk kabel som överskrider Finlands gräns varierar typiskt mellan färre än tio par och flera hundra par. Ett enskilt fiberpar kan genom den våglängdsteknik som i dag allmänt an-

vänds förmedla cirka 90 våglängder, dvs. kanaler. En enskild kanal kan överföra 100–400 gigabit per sekund (Gbit/s) beroende på vilken teknik som används och hur lång överföringssträckan är. Den maximala överföringskapaciteten för enskilda fiberpar varierar, men kan med den teknik som typiskt används i dag vara cirka 18 terabit per sekund (Tbit/s) i internationella förbindelser. En enskild optisk kabels maximala överföringskapacitet beror på hur många fiberpar den innehåller.

Utifrån det som ovan sagts om datatrafik till och från Finland och datatrafik som går via Finland kan man se att mängden överförda data är tämligen stor, även om underrättelseinhämtningen som avser datatrafik riktas mot en våglängd. Det går dock att ur dataflödet vid exempelvis en viss våglängd gallra ut data som är irrelevant för underrättelseinhämtningen. Enligt uppskattningar av de största företag som utvecklar datanätteknik var cirka 66 procent av datatrafiken 2016 relaterad till videotjänster (t.ex. Netflix, HBO, Youtube) eller musiktjänster (t.ex. Spotify). Enligt företagens bedömning kommer överföringen av videomaterial att år 2021 stå för cirka 80 procent av all datatrafik. Dessutom kan man ur dataflödet utesluta exempelvis den datatrafik som genereras av nätbutikerna. Den utgör enligt uppskattningar cirka 6,5 av all datatrafik.

Efter dessa uteslutningar kan den underrättelseinhämtning som avser datatrafik antas rikta sig mot cirka 15 av all datatrafik, det vill säga i praktiken 15 procent av den data som överförs exempelvis vid en viss våglängd. De sökvillkor som anges i tillståndet från domstolen riktas till denna andel. Utifrån sökvillkoren kan det i det enskilda fallet uppskattas att cirka 0,5 procent av datatrafiken, det vill säga cirka 0,75 gigabit per sekund av alla överförda data, blir föremål för underrättelseinhämtning.

Den data som selekterats genom sökvillkoren analyseras, och överflödig information utplånas med stöd av skyldigheten till omedelbar utplåning Det innebär att endast en liten del av den mängd data som motsvarar sökvillkoren till sist och syvende sparas i de rapporter och sammandrag som görs upp med anledning av underrättelseinhämtningsuppdraget. Därutöver sparas i enlighet med sökvillkoren fortsättningsvis identifikationsuppgifter och andra uppgifter som anknyter till underrättelseinhämtningsuppdraget. På grundval av dem kan den underrättelseinhämtning som avser datatrafik och annan underrättelseverksamhet ges en ny inriktning.

4.5 Bedömning av för- och nackdelarna med lagstiftningen om civil underrättelseinhämtning

Berättigandet för det underrättelsesystem som bygger på underrättelselagstiftningen är till stor del beroende av hur väl och till vilka kostnader systemet klarar av att nå de mål som satts för det. Vid bedömningen av detta berättigande spelar avvägningen mellan de eventuella för- och nackdelar som hänför sig till underrättelselagstiftningen en central roll. Frågan är utpräglat situationsbunden, men dess kärninnehåll är oförändrat: för- och nackdelarna med användningen av underrättelsesystemet måste jämföras och fördelarna måste vara större än nackdelarna.

Avvärjande av hot

Underrättelselagstiftningen gör det möjligt att utforma en aktuell lägesbild av säkerhetssituationen, förbereda sig på allvarliga hot mot den nationella säkerheten och avvärja hot. Eftersom underrättelseinhämtningens grundläggande uppgift är att skydda den demokratiska stats- och samhällsordningen, samhällets vitala funktioner, ett stort antal människors liv eller hälsa samt den internationella freden och säkerheten mot hot som riktas mot dem, är den första och viktigaste praktiska fördelen som eftersträvas med underrättelseregleringen att avvärja sådana hot. Genom att undvika att hoten realiseras försöker man undanröja eller åtminstone minska de direkta och indirekta följderna av ett realiserat hot. Direkta följder som genast yppar sig är

till exempel förlust av människors liv och hälsa och materiella skador. Exempelvis till följd av terroristattacken i Norge i juli 2011 har de direkta städ- och reparationskostnaderna för det skadade regeringskvarteret samt kostnaderna för anskaffning av tillfälliga lokaler och ökad säkerhetsbevakning uppskattats till 1,45 miljarder norska kronor, vilket motsvarar cirka 150 miljoner euro (Minister Aasrud, Rigmor: intervju i Aftenposten). Indirekta följder som syns med en viss fördröjning är till exempel skador för den internationella handeln, turismen och försäkringsbranschen, marknadsstörningar samt skärpta kriminal- och säkerhetspolitiska åtgärder och ökningar på utgiftssidan i statsbudgeten. Till exempel i samband med den så kallade bronsstatykonflikten 2007 slogs såväl bankernas nättjänster som mediernas och statens webbplatser ut i en omfattande nätattack riktat mot Estland. Även om det inte finns mycket information tillgänglig om kostnaderna för attacken meddelade en estnisk bank att de ekonomiska skadorna uppgick till ungefär 1 miljon amerikanska dollar (Herzog, Stephen: Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses).

Brottsbekämpning

Underrättelselagstiftningen antas främja förundersökningsmyndigheternas och andra behöriga myndigheters möjligheter att få information om de allvarligaste brotten. Med den föreslagna regleringen kan man i enskilda fall bättre förhindra att situationen utvecklas från förberedelse för ett allvarligt brott till genomförande av brottet. Lagarbetsgruppen för civil underrättelseinhämtning har i sitt betänkande uppskattat att i samband med skyddspolisens underrättelseinhämtning framkommer varje år två grova brott som leder till förundersökning och flera allvarliga brott som fortfarande går att förhindra. En annan, men likaså viktig fördel med underrättelseregleringen, hänför sig således till brottsbekämpningen, dvs. målet att förebygga brott eller ställa de skyldiga till straffrättsligt ansvar. Genom brottsbekämpning försöker man minska de negativa följderna av straffbart beteende, såsom personskador på brottsoffer, lidande, sakskador och ekonomiska skador och kostnader för statens kontrollsystem. De totala kostnaderna för ett brott som begåtts i terroristiskt syfte kan även samhällsekonomiskt bli betydande och uppgå till flera miljoner euro.

De totala kostnaderna för ett brott som begåtts i terroristiskt syfte kan bli samhällsekonomiskt betydande och uppgå till flera miljoner euro. Exempelvis de terroristattacker som inträffat i Frankrike har enligt de franska myndigheterna orsakat Frankrike förluster på uppskattningsvis 750 miljoner euro i form av minskad turism (Reuters in Paris 23.8.2016). Terroristattackerna i Bryssel uppskattas ha kostat den belgiska ekonomin nästan en miljard (Politico 26.7.2016). Enligt en uppskattning som International Air Transport Association (IATA) framförde i en rapport som publicerades i maj 2017 minskade de terroristattacker som genomfördes i Västeuropa i slutet av 2015 och början av 2016 de europeiska flygbolagens internationella passagerartrafik och försämrade de europeiska flygbolagens omsättning med cirka 2,5 miljarder dollar 2016.

Direkta kostnadseffekter

Underrättelseregleringen kommer att ha effekter på statsbudgeten. Skyddspolisens omkostnader med tyngdpunkt på initialfasen – före det år då lagstiftningen om civil underrättelseinhämtning träder i kraft – har uppskattats till 12,5 miljoner euro, varav 9,7 miljoner euro går till investeringar av engångsnatur. De följande åren har skyddspolisens tilläggsomkostnader för regleringen om civil underrättelseinhämtning och den civila underrättelseförmågan uppskattats landa på nivån 11 miljoner euro. Då förklaras utgifterna med framför allt personalkostnader, operativa utvecklingskostnader och kostnader för underhåll av informationssystemen. Den övriga polisens, inrikesministeriets och justitieförvaltningens årliga omkostnader för civil underrättelseinhämtning har uppskattats till sammanlagt cirka 2,6 miljoner euro från och med det år

då lagen föreslås träda i kraft. Till grund för den förstnämnda omkostnadshelheten ligger avvärjandet av hot medan brottsbekämpningen ligger till grund för den sistnämnda.

Botten-upp-anmärkningar

Fördelarna med underrättelselagstiftningen är ovan indelade i avvärjande av hot och brottsbekämpning och nackdelarna i begränsningar av verksamheten och lidande samt direkta kostnadseffekter. Eftersom hoten är mångahanda och föränderliga över tiden, varierar också de direkta och indirekta kostnadseffekterna stort om hoten realiseras och är svåra att förutsäga. Fördelarna med brottsbekämpning varierar enligt hur många och vilka slags brottsärenden som varje år kan anmälas till förundersökningsmyndigheterna och andra behöriga myndigheter på grund av underrättelseinhämtningen. Det står dock klart att sannolikheten att avvärja hot mot den nationella säkerheten och brott som framkommer i samband med den civila underrättelseinhämtningen är desto större i ju högre grad denna avvärjningsförmåga tilldelas resurser. I ljuset av de föregående exemplen står det också klart att de kostnader för skador som man sparar genom att lyckas avvärja redan ett hot kan vara mångfaldiga i förhållande till de årliga omkostnaderna för underrättelseförmågan. De fördelar som uppnås genom underrättelsereglering och underrättelseförmåga kan således förutspås övergå nackdelarna inte bara i en jämförelse mellan de svårvärderade skyddsintressena och begränsningarna av verksamheten, utan också ekonomiskt.

5 Beredningen av propositionen

5.1 Beredningsskeden och beredningsmaterial

Cybersäkerheten aktualiserades redan 2010 i säkerhetsstrategin för samhället (Statsrådets principbeslut 16.12.2010). Cyberhot identifierades som ett potentiellt hot och det konstaterades att intrång i informationssystem under vissa förhållanden rent av kan motsvara kännetecknen på användningen av militära maktmedel. I strategin för cybersäkerheten i Finland (Statsrådets principbeslut 24.1.2013) anges de centrala målen och riktlinjerna för verksamheten, med vilkas hjälp man kan svara på utmaningarna i cyberomgivningen och säkerställa att den fungerar.

Enligt punkt 5 i riktlinjerna i cybersäkerhetsstrategin bildas den militära cyberförsvarsförmågan av kapaciteterna underrättelse, påverkan och skyddande. För att säkerställa kapaciteten utvecklas underrättelse- och påverkansförmågan i cyberomgivningen som en del av utvecklandet av den övriga användningen av militära maktmedel.

Republikens president och statsrådets utrikes- och säkerhetspolitiska ministerutskott diskuterade på sitt möte den 7 november 2013 informationssäkerheten inom statsförvaltningen samt behoven av att utveckla den nationella cybersäkerheten. Saken hade behandlats tidigare bland annat på ett möte i maj 2013. I enlighet med den diskussion som fördes då och strategin för cybersäkerheten i Finland, som publicerats i form av statsrådets principbeslut den 24 januari 2013, har försvarsförvaltningen granskats den internationella rättens och den nationella lagstiftningens tillämplighet och tillräcklighet och även vissa andra länders lagstiftning som inverkar på cybersäkerheten.

Försvarsministeriet tillsatte den 13 december 2013 en arbetsgrupp för att utveckla lagstiftningen i syfte att förbättra säkerhetsmyndigheternas förmåga att inhämta information. Målet var att utreda säkerhetsmyndigheternas verksamhetsbetingelser när det gäller informationsinhämtning särskilt med beaktande av de hot som riktas mot Finland via cyberomgivningen samt de nuvarande befogenheterna för informationsinhämtning och behoven av att utveckla dem. Arbetsgruppen granskade i sitt arbete befogenhetsbehoven i anslutning till såväl civil

som militär underrättelseinhämtning. För de civila myndigheternas del låg tyngdpunkten i arbetsgruppens arbete på skyddspolisens uppgifter och befogenheter. Arbetsgruppen överlämnade sitt betänkande till försvarsministeriet den 14 januari 2015 (Riktlinjer för en finsk underrättelselagstiftning. Betänkande av arbetsgruppen för en informationsanskaffningslag). I betänkandet bedöms i synnerhet behoven av att utveckla underrättelselagstiftningen.

Arbetsgruppen för en informationsinhämtningslag föreslog att för att skapa en författningsgrund som gäller underrättelseinhämtning skulle ett eller flera lagstiftningsprojekt inledas, som kan beredas inom de olika ansvarsområdena. Det borde också övervägas om beredningen kunde vara till exempel parlamentarisk eller annars ske under politisk styrning.

Betänkandet av arbetsgruppen för en informationsinhämtningslag sändes på remiss den 9 februari 2015 och 150 olika instanser ombads yttra sig. Begäran om yttrande var också tillgänglig för allmänheten på försvarsministeriets webbplats. Dessutom ombads professor Martin Scheinin från European University Institute, biträdande professor Juha Lavapuro från Tammerfors universitet och professor Tomi Voutilainen från Östra Finlands universitet yttra sig särskilt. 74 instanser yttrade sig. Ett sammandrag av yttrandena har utarbetats (försvarsministeriets publikation FI.PLM.2015-3439). I responsen i yttrandena anslöt sig remissinstanserna i stor utsträckning till den bedömning av omvärldens förändring i ett digitaliserat samhälle med datanät som utgjorde utgångspunkt för betänkandet. Luckorna i dagens lagstiftning sågs som ett problem och det ansågs motiverat att skapa en författningsgrund. Meningarna var dock delade om de utvecklingsförslag och slutsatser som presenterats i betänkandet. Det ansågs problematiskt att samordna spänningen mellan myndigheternas behov av information och skyddet för privatlivet.

Enligt programmet för statsminister Juha Sipiläs regering (SRM 1/2015 rd) kräver de ökande riskerna och nya hoten beredskap och förberedelser av ett nytt slag av hela samhället. Regeringen kommer att stärka det övergripande säkerhetstänkandet nationellt, inom EU och inom ramen för det internationella samarbetet. Detta gäller framför allt nya och omfattande hot som påverkansåtgärder av hybridkaraktär, cyberattacker och bekämpning av terrorism. Regeringen kommer att stärka de inre förutsättningarna för den yttre säkerheten. Regeringen föreslår att underrättelse utomlands och datatrafikspaning ska basera sig på lagstiftning. Vid beredningen av denna lagstiftning ska tillgodoseendet av de grundläggande fri- och rättigheterna och de mänskliga rättigheterna beaktas.

Lagstiftningsprojektet som gäller underrättelseinhämtning behandlades på regeringens strategimöte den 20 augusti 2015. Under mötet beslöt man att inrikesministeriet leder projektet som gäller civil underrättelseinhämtning och försvarsministeriet projektet som gäller militär underrättelseinhämtning medan justitieministeriet leder det projekt som gäller eventuella ändringar i grundlagen. Den militära underrättelseinhämtningen och bestämmelserna om civil underrättelseinhämtning, som bereds samtidigt vid inrikesministeriet, ska vara samordnade.

Inrikesministeriet tillsatte den 1 oktober 2015 ett projekt som fick i uppdrag att bereda förslag till lagstiftning om civil underrättelseinhämtning, som skulle utgöra författningsgrund för personbaserad underrättelseinhämtning som avser utländska förhållanden, underrättelseinhämtning som avser datasystem och underrättelseinhämtning som avser datatrafik. Dessutom var en uppgift att utreda och bedöma hur skyddspolisens hemliga metoder för inhämtande av information fungerar och om de är tillräckliga samt att utreda och bedöma olika sätt och alternativ att inhämta underrättelseinformation. Samtidigt bereds andra behövliga förslag till ändringar i lagstiftning med anknytning till projektet.

Det viktigaste syftet med projektet är att förbättra den nationella säkerheten. Målet är att bereda centrala bestämmelser om civil underrättelseinhämtning och på så sätt förbättra skydds-

polisens informationsinhämtning om allvarliga internationella hot så att skyddspolisen har befogenheter för personbaserad underrättelseinhämtning som avser utländska förhållanden och underrättelseinhämtning som avser datasystem samt underrättelseinhämtning som avser datatrafik.

I lagarbetsgruppen för civil underrättelseinhämtning ingick medlemmar som företrädde presidentens kansli, justitieministeriet, försvarsministeriet, inrikesministeriet, skyddspolisen, polisstyrelsen, centralkriminalpolisen samt experter som företrädde Finlands näringsliv, statsrådets kansli, utrikesministeriet, kommunikationsministeriet samt Huvudstabens underrättelseavdelning. Arbetsgruppen överlämnade ett enhälligt förslag.

I den slutrapport som arbetsgruppen som utrett skyddspolisens administrativa ställning och resultatstyrning publicerade den 24 september 2014 (Slutrapport av den arbetsgrupp som haft till uppgift att utreda skyddspolisens administrativa ställning, resultatstyrning samt utveckling av övervakningen, Inrikesministeriets publikation 28/2014) konstateras det att om skyddspolisens uppgifter och befogenheter utvecklas i en riktning som betonar underrättelseinhämtning, uppstår det ett behov att omarbeta formerna för den externa laglighetsövervakningen och den parlamentariska kontrollen. Det kan till exempel vara fråga om att det förutsätts nya domstolstillstånd och att ett särskilt parlamentariskt kontrollorgan inrättas. Om betydelsen av de underrättelseinhämtningselement som avser utländska förhållanden ökar ytterligare i skyddspolisens verksamhet, borde regleringen, styrningen och övervakning av den civila och den militära underrättelseinhämtningen utvecklas så att de beaktar varandra. I arbetsgruppens slutrapport konstateras vidare att om skyddspolisens underrättelsebefogenheter utökas, borde man överväga att begränsa skyddspolisens förundersökningsuppgifter och förundersökningsbefogenheter i syfte att trygga en rättvis rättegång. Skyddspolisen kunde fortfarande enligt behov delta i förundersökningen i egenskap av sakkunnigmyndighet.

Den expertarbetsgrupp som justitieministeriet tillsatt hade i uppdrag att utreda och bereda en översyn av grundlagen så att det genom lag kan föreskrivas om begränsningar i skyddet för förtroliga meddelanden för att skydda den nationella säkerheten när nödvändiga förutsättningar för detta anses föreligga. Vid beredningen skulle Finlands internationella människorättsförpliktelser beaktas. Arbetsgruppen publicerade sitt betänkande den 11 oktober 2016. Arbetsgruppen föreslog i sitt betänkande att 10 § i grundlagen skulle ändras så att till den fogas ett nytt 4 mom., där förutsättningarna för att begränsa hemligheten i fråga om förtroliga meddelanden samlas. Enligt förslaget kan genom lag bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång, säkerhetskontroll och under frihetsberövande för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten.

Inrikesministeriet tillsatte formellt en parlamentarisk uppföljningsgrupp för projekten i anslutning till reformen av underrättelselagstiftningen. Gruppen fungerar som länk mellan lagstiftningsprojekten och riksdagen, för att riksdagen hela tiden ska vara medveten om hur projekten framskrider. Uppföljningsgruppen mandattid var från den 11 december 2015 till den 31 december 2016. Uppföljningsgruppens mandattid förlängdes till utgången av 2017 och dess uppdrag sågs över.

I underrättelselagstiftningens tidigare faser har man upptäckt att underrättelseinhämtningen kräver behörig, oberoende extern övervakning. Detta framgår också av Europadomstolens avgörandepraxis. För att organisera övervakningen av säkerhetsmyndigheternas underrättelseinhämtning tillsatte justitieministeriet den 17 oktober 2016 en arbetsgrupp som fick i uppdrag att bereda lagstiftning för övervakning av de civila och de militära underrättelsemyndigheternas underrättelseverksamhet.

5.2 Remissyttranden och hur de har beaktats

Lagarbetsgruppen för civil underrättelseinhämtning överlämnade sitt betänkande (Lagstiftning om civil underrättelseinhämtning, Betänkande av lagarbetsgruppen för civil underrättelseinhämtning, Inrikesministeriets publikation 8/2017) till inrikesministeriet Paula Risikko den 19 april 2017. Arbetsgruppen föreslog att det stiftas en ny lag om civil underrättelseinhämtning avseende datatrafik samt att polislagen ändras så att till den fogas ett nytt 5 a kap., där det föreskrivs om metoder för underrättelseinhämtning och användning av dem inom civil underrättelseinhämtning. Dessutom föreslår arbetsgruppen ändringar i polisförvaltningslagen, lagen om behandling av personuppgifter i polisens verksamhet, förundersökningslagen, tvångsmedelslagen och lagen om offentlighet vid rättegång i allmänna domstolar.

Förslaget sändes på remiss den 24 april 2017. Remisstiden var åtta veckor (24.4–16.6.2017). Yttrande begärdes av följande instanser: Ålands förvaltningsdomstol, Ålands landskapsregering, American Chamber of Commerce in Finland (AmCham Finland), Amnesty International – Finländska sektionen, Auktoriserade Jurister, BaseN Ab, Cinia Ab, CSC-Tieteen tietotekniikan Keskus Oy, Rättspolitiska föreningen Demla rf, DNA Abp, riksdagens justitieombudsmans kansli, Electronic Frontier Finland ry Effi, Finlands näringsliv EK, Elisa Abp, Enfo Oyj, Ericsson, FiCix ry, Finnet-förbundet rf, Finnvera, FISC, F-Secure Oyj, Fujitsu Finland Oy, Google, Helsingfors förvaltningsdomstol, Helsingin tingsrätt, Försörjningsberedskapscentralen, Tavastehus förvaltningsdomstol, Förbundet för mänskliga rättigheter, Internet-käyttäjät ikuisesti - IKI ry, Invest in Finland, Finpro ry, Östra Finlands förvaltningsdomstol, Förhandlingsorganisationen för offentliga sektorns utbildade FOSU rf, Opinionsnämnden för massmedier, Förbundet för den offentliga sektorn och välfärdsområdena JHL rf, Juridiska Föreningen i Finland, delegationen för medborgarsamhällspolitik, Nationella Samlingspartiet r.p., Centralhandelskammaren, Centralkriminalpolisen, högsta förvaltningsdomstolen, högsta domstolen, kommunikationsministeriet, jord- och skogsbruksministeriet, Migrationsverket, Microsoft Oy, Nixu Oy, Nokia Abp, Ohjelmistoyrittäjät ry, justitiekanslersämbetet, justitieministeriet, undervisnings- och kulturministeriet, Löntagarorganisationen Pardia rf, Patria Abp, Sannfinländarna r.p, Piratpartiet r.p., Norra Finlands förvaltningsdomstol, Polisyrkeshögskolan, Polisstyrelsen, försvarsministeriet, huvudstaben, Staben för gränsbevakningsväsendet, social- och hälsovårdsväsendet, SSH Secure Communications Oyj, Skyddspolisen, Finlands Advokatförbund, Suomen Erillisverkot Oy, Suomen Internet-yhdistys, Finlands Journalistförbund, Centern i Finland r.p., Kristdemokraterna i Finland (KD) r.p., Finlands Juristförbund, Svenska folkpartiet i Finland r.p., De Hundras Kommitté i Finland rf, Finlands Socialdemikratiska Parti r.p., republikens presidents kansli, Teknologiindustrin rf, Telia Finland Oyj, Tieto Finland Oyj, Tieto- ja viestintätekniikan ammattilaiset TIVIA ry, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Dataombudsmannens byrå, Utvecklingscentralen för Informationssamhälle rf TIEKE, Tullen, Åbo förvaltningsdomstol, Sekretariatet för säkerhetskommittén, arbets- och näringsministeriet, utrikesministeriet, Vasa förvaltningsdomstol, Riksåklagarämbetet, statsrådets kansli, finansministeriet, Vänsterförbundet r.p., Mediernas Centralförbund, Kommunikationsverket, Gröna förbundet r.p. (riksdagsgruppen), miljöministeriet.

Största delen av yttrandena finns att läsa på adressen http://valtioneuvosto.fi/hankkeet (projektregisternummer SM047:00/2015). Ett sammandrag av yttrandena publicerades den 7 september 2017 (Lagstiftning om civil underrättelseinhämtning, Sammandrag av remissvaren, Inrikesministeriets publikation 21/2017).

Begäran om yttrande sändes till 96 instanser, varav 59 yttrade sig. Förutom remissinstanserna yttrade sig sju andra, så sammanlagt 66 instanser yttrade sig om utlåtandet.

I yttrandena kommenterades arbetsgruppens betänkande ingående. Största delen av remissinstanserna ansåg att den nya lagstiftningen om civil underrättelseinhämtning och stiftandet av

den är nödvändigt och värt att understöda. I rätt många yttranden kritiserade man inte paragraferna, utan önskade att motiveringen till dem skulle preciseras. En minoritet av remissinstanserna förhöll sig kritiskt till förslaget.

Responsen i yttrandena beaktades i stor utsträckning i den fortsatta beredningen av lagarna. I synnerhet motiveringen till paragraferna preciserades och utökades. I flera yttranden fästes uppmärksamhet vid inriktningen av underrättelseinhämtning som avser datatrafik och man efterlyste noggrannare avgränsning eller mer avgränsad teknik. Utifrån yttrandena utarbetades för konsekvenserna för informationssamhället en grundlig redogörelse för hur underrättelseinhämtning som avser datatrafik riktar sig mot datatrafiken i kommunikationsnät.

Lagarbetsgruppen för civil underrättelseinhämtning föreslog att det i 5 a kap. 3 § föreskrivs om föremålen för civil underrättelseinhämtning. I 3 § i lagen om civil underrättelseinhämtning avseende datatrafik ingår samma hotförteckning med tio punkter. Paragrafen är mycket viktig, eftersom den på ett uttömmande sätt anger om vilken verksamhet som allvarligt hotar den nationella säkerheten man får inhämta information med underrättelseinhämtningsmetoder. Rätt många instanser, såsom justitieministeriet, Advokatförbundet, Demla, Finlands journalistförbund och Amnesty International Finländska sektionen ansåg i sin respons att det måste satsas ytterligare på att definiera och noggrant avgränsa hoten.

Utifrån responsen i yttrandena preciserades och avgränsades grunderna för användning av underrättelseinhämtningsmetoderna noggrant så att det företogs preciserande, delvis tekniska ändringar i utformningen av föremålen. Paragrafens 3 punkt (verksamhet som hotar stats- och samhällsordningen) ändrades till verksamhet som hotar den demokratiska samhällsordningen. Till paragrafen fogades dessutom en ny 10 punkt om verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och deltar i annan internationell verksamhet.

Den viktigaste ändringen var att de föremål som avses i paragrafen inte i sig anses berättiga till användning av en underrättelseinhämtningsmetod, utan beträffande varje föremål för civil underrättelseinhämtning ska den civila underrättelsemyndigheten i det enskilda fallet kunna påvisa att den verksamhet som avses i punkten i fråga utgör ett allvarligt hot mot den nationella säkerheten. Denna förutsättning framgår av 5 a kap. 4 § 1 mom., enligt vilket: ”En allmän förutsättning för att en metod för underrättelseinhämtning ska få användas är att man med den med fog kan antas få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten.” Det är fråga om en klar förutsättning för att få använda en metod, som också förutsätter att existensen av de ovannämnda omständigheterna motiveras. Förutsättningarna för att få utöva befogenheter preciserades och avgränsades noggrannare även i övrigt utifrån responsen genom att det i detaljmotiveringen skrevs in omständigheter som begränsar den civila underrättelsemyndighetens prövningsrätt och som hänför sig till de allmänna polisrättsliga principerna i början av polislagen som styr användningen av befogenheterna till underrättelseinhämtning.

När det gäller den laglighetsövervakning (och parlamentariska kontroll) som riktar sig mot den civila underrättelseverksamheten behandlades övervakningens och kontrollens viktiga roll i flera yttranden. Laglighetsövervakningen och den parlamentariska kontrollen ska vara effektiv, trovärdig och ordnad på behörigt sätt. Enligt förslaget från lagarbetsgruppen för civil underrättelseinhämtning skulle skyddspolisen ha informerat tillsynsmyndigheten för underrättelseinhämtning om domstolens tillstånd så snart som möjligt efter domstolens beslut. Denna skyldighet utvidgades till att gälla varje beslut om användning av en underrättelseinhämtningsmetod samt beslut om skyddande av civil underrättelseinhämtning, yppandeförbud eller uppskjutande av en anmälan som avses i 44 § 1 mom. Även det bemyndigande att utfärda förordning som anges i de närmare bestämmelserna utvidgades för statsrådets del till att gälla det förfarande som gäller överföring av en uppgift som ska lämnas ut till brottsbekämpningen och

de behövliga uppgifter som ska ges i samband med detta, organiserandet av samarbetet mellan skyddspolisen och militärunderrättelsemyndigheten, organiserandet av samarbetet mellan skyddspolisen och andra myndigheter, organiserandet av samordningen av den hemliga informationsinhämtningen och organiserandet av samordningen av underrättelseverksamheten. Genom förordning av inrikesministeriet får det utfärdas bestämmelser om organiserandet av övervakningen av den civila underrättelseverksamheten inom inrikesförvaltningen, organiserandet av samarbetet mellan skyddspolisen och den övriga inrikesförvaltningen samt om organiserandet av skyddspolisens internationella samarbete.

I responsen behandlades arbetsgruppens förslag om utlämnande av information för brottsbekämpning (5 a kap. 43 § i polislagen) i ganska stor utsträckning. Strävan har varit att beakta responsen i yttrandena framför allt i motiveringen, men även i paragrafen företogs ändringar som hänför sig till prövningen i anslutning till de anmälningar som avses i paragrafen.

Frågorna om tillgodoseende av de grundläggande fri- och rättigheterna samt de mänskliga rättigheterna väckte i någon mån diskussion i förhållande till responsen som helhet. Till denna del fästes under beredningen särskilt uppmärksamhet vid avsnittet ”Förhållande till grundlagen samt lagstiftningsordning” i propositionen, men grundlagsfrågor behandlas mer ingående även i detaljmotiveringen till befogenhetsparagraferna.

I några utlåtanden dryftades den civila underrättelseinhämtningens effektivitet. Under den fortsatta beredningen presenterades dessutom det avsnitt som gäller propositionens konsekvenser för det oberoende och självständiga rådet för bedömning av lagstiftningen, som verkar i anslutning till statsrådets kansli. Utifrån responsen utarbetades särskilt för avsnittet om konsekvenser för informationssamhället en bedömning av hur underrättelseinhämtning som avser datatrafik riktar sig mot datatrafiken i kommunikationsnät. För propositionens konsekvenser utarbetades dessutom ett nytt avsnitt där man väger för- och nackdelarna med lagstiftningen om civil underrättelseinhämtning.

Propositionens avsnitt om ekonomiska konsekvenser kommenterades i flera yttranden. Under den fortsatta beredningen företogs ändå inga ändringar i det.

Under den fortsatta beredningen av förslaget till lagstiftning om civil underrättelseinhämtning fästes uppmärksamhet vid enhetligheten mellan lagförslagen om civil och militär underrättelseinhämtning och de förenhetligades i samarbete mellan inrikesministeriet och försvarsministeriet i alla avseenden där sådan samordning är motiverad och önskvärd med tanke på en klar och tydlig reglering.

Utifrån responsens företogs rikligt med tekniska ändringar i såväl paragraferna som motiveringen, motiveringen fördjupades och utvidgades till exempel i fråga om bedömningen av överensstämmelsen med grundlagen. Språket i lagförslagen och motiveringen finslipades på många punkter.

Utlåtande av rådet för bedömning av lagstiftningen

Propositionsutkastet har behandlats av rådet för bedömning av lagstiftningen, som lämnat utlåtande i ärendet (http://vnk.fi/documents/10616/2913095/Lausunto+siviilitiedustelulaista+21.12.2017/30b6f3de-79e1-47c4-ac17-1fcd390bdcd4, på finska).

Rådet för bedömning av lagstiftningen anser i sitt utlåtande om utkastet till proposition med förslag till lagstiftning om civil underrättelseinhämtning att utkastet huvudsakligen har beretts omsorgsfullt. Enligt rådet bör propositionen emellertid presentera mer exakta kvantitativa be-

dömningar av storleksklassen på säkerhetshoten. Dessutom bör konsekvensbedömningarna utvidgas och preciseras och en konkret plan presenteras om utvärderingen i efterskott och om uppföljningen.

Enligt rådet är de viktigaste utvecklingsobjekten i utkastet till proposition följande: 1) Proposition bör presentera mer exakta bedömningar av storleksklassen på reformens fördelar och kostnader, i synnerhet ur hushållens och företagsverksamhetens synvinkel, 2) underrättelseverksamhetens vidare internationella utveckling och kärnområden ägnas i utkastet endast liten uppmärksamhet; det bör ges en närmare motivering till varför just de länder som ingår i den internationella översikten har valts ut, 3) av de ersättningar som betalas till företag av statens medel bör det anges åtminstone en ungefärlig kvantitativ bedömning, och 4) propositionen bör innehålla en närmare beskrivning av reformens konsekvenser för andra myndigheter, i synnerhet för centralkriminalpolisen.

Det centrala syftet med lagstiftningen om civil underrättelseverksamhet är att förbättra den nationella säkerheten och att skapa en rättslig grund för underrättelseinhämtning. Projektet hänger nära samman med de lagstiftningsprojekt om militär underrättelseinhämtning och om övervakningen av underrättelseverksamhet som försvarsministeriet respektive justitieministeriet bereder. Propositionerna om dessa ämnen kommer att lämnas till riksdagen samtidigt som denna proposition. Syftet med lagförslagen om inhämtning av underrättelser är att ge bättre verksamhetsförutsättningar för inhämtningen. Justitieministeriets proposition kommer att innehålla förslag om extern laglighetsövervakning av civil och militär underrättelseinhämtning och om vissa detaljer i fråga om den parlamentariska tillsynen.

Rådet för bedömning av lagstiftningen påpekar att reformen beretts genom flera olika separata utkast till proposition och att den därför är krävande när det gäller att bedöma dess konsekvenser. Utkastet bör tydligt ange både konsekvenserna av varje enskild proposition och de samlade konsekvenserna av reformen. När projektet inleddes utvärderades olika lagstiftningstekniska lösningar och bland annat funktionella skäl ledde till att lagstiftningspaketet delades upp i tre separata projekt för civil underrättelseinhämtning, militär underrättelseinhämtning respektive ändring av grundlagen. Den del som gäller övervakning av underrättelseinhämtningen avskildes till ett eget projekt. Lagförslagen ingår i olika propositioner men utgör en helhet i fråga om konsekvensbedömning. Samtidigt är bedömningen av konsekvenserna av varje proposition specifik och baserad på de föreslagna lagarna i den berörda propositionen. Exempelvis gäller bedömningen av konsekvenserna av justitieministeriets proposition lagförslagen om övervakning av underrättelseverksamheten. Tidsplanen för dessa lagförslag bestämdes så att de ska behandlas samtidigt i riksdagen, och på så sätt är det också möjligt att få grepp om helheten med tanke på konsekvensbedömningen.

I denna proposition presenteras de föreslagna åtgärdernas direkta konsekvenser för statsbudgeten så exakt som möjligt utifrån den tillgängliga informationen. Det finns skäl till försiktighet när det gäller att göra kvantitativa bedömningar av konsekvenserna för företagsverksamheten, eftersom sådana bedömningar kan ge vilseledande resultat. Rent allmänt kan man exempelvis göra den bedömningen att ändrad lagstiftning leder till att arbetet inom teleföretagen kan komma att öka men att de allt längre tillståndstiderna i fråga om metoderna för underrättelseinhämtning kan stävja ökningen. Vid en mer långvarig insats för underrättelseinhämtning skulle detta minska belastningen av teleföretagens personalresurser i förhållande till om tillstånden bara gällde en månad. Men samtidigt inbegriper bedömningen av de ekonomiska konsekvenserna en verbal beskrivning med angivande av belopp och en sammanfattande tabell av de ekonomiska konsekvenserna för skyddspolisen. Utgifterna i fråga inbegriper också en uppskattning av de ersättningar som betalas till företag och uppgifterna om den exakta fördelningen av det beloppet är inte offentliga till följd av uppskattningarna om antalet tillstånd som gäller metoderna för underrättelseinhämtning.

Rådet för bedömning av lagstiftningen pekar också på att utkastet till proposition inte presenterar någon bedömning av vilken ekonomisk betydelse hot mot den nationella säkerheten såsom it-brottslighet och terrorism har ur hushållens synvinkel. Det primära syftet för lagstiftningsprojekten är inte att bekämpa brottslighet även om detta skulle bli en indirekt effekt av lagstiftningen. Med andra ord syftar konsekvensbedömningen inte till att belysa de presenterade frågekomplexen ur brottsbekämpningsperspektiv. Syftet är att lagstiftningen om underrättelseinhämtning ska förbättra det finländska samhällets möjligheter att skydda sig mot allvarliga hot mot den nationella säkerheten och fungera som stöd för den högsta statsledningens beslutsfattande och säkerställa att besluten bygger på korrekta, uppdaterade och tillförlitliga uppgifter. Vidare kan exempelvis dåd i terroristiskt syfte se ut på så många olika sätt att en kvantitativ bedömning ur hushållens synvinkel kan variera stort. Exempelvis beror variationsintervallet för de ekonomiska konsekvenserna uttryckt i euro på vad terrorattacken utförs med – ett stålvapen, en lastbil, ett flygplan, en sprängladdning. Utöver redskapet inverkar också till exempel målet för dådet. Bedömning av sådana kostnadseffekter, såväl direkta som indirekta, är dessutom i fråga om andra objekt för civil underrättelseinhämtning inte möjlig när verksamheten är fullständigt oförutsägbar. Därför är det i detta avseende endast i vid analys i efterskott möjligt att fallspecifikt göra en bedömning av hurdana konsekvenserna blev och hurdana belopp som eventuellt kunnat sparas.

I den del som gäller propositionens konsekvenser för brottsbekämpning konstateras det att de föreslagna lagarna antas främja förundersökningsmyndigheternas och andra behöriga myndigheters möjligheter att få information om de allvarligaste brotten. Med den föreslagna regleringen kan man i enskilda fall bättre förhindra att situationen utvecklas från förberedelse för ett allvarligt brott till att brottet begås. Lagarbetsgruppen för civil underrättelseinhämtning har i sitt betänkande uppskattat att i samband med skyddspolisens underrättelseinhämtning varje år framkommer två grova brott som leder till förundersökning och flera allvarliga brott som fortfarande går att förhindra. Det är inte ändamålsenligt att göra kvantitativa analyser av förhindrade brott eftersom objekten för civil underrättelseinhämtning är så pass olika. Information som erhållits med hjälp ab befogenheterna för underrättelseinhämtning analyseras och sänds till den högsta statsledningen eller andra myndigheter för kännedom. På detta sätt kommer det att gå att i ett mycket tidigt skede reagera också på sådana hot mot den nationella säkerheten som om de framskrider kan utgöra brott. Detta kommer emellertid att ske i en fas där det inte ens i praktiken är möjligt att ge en grov uppskattning av antalet brott som eventuellt förhindrats eller om brottstyperna.

Rådet för bedömning av lagstiftningen anser att den del som gäller internationell praxis bör innehålla en motivering till varför just de länder som presenterats valts ut för jämförelse och hur exempel från och reformer i andra länder har påverkat de åtgärder som föreslås i propositionsutkastet. Det framgår av utkastet att flera länder lagstiftat om underrättelseverksamhet de senaste åren, men det förblir oklart för läsaren vilken riktning i vilken riktning regleringen går i och vilka olika strategier som finns.

I avsnittet med den internationella jämförelsen behandlas lagstiftningen om civil och militär underrättelseinhämtning i Norge, Danmark och Tyskland ämnesvis. I försvarsministeriets proposition som gäller lagstiftningen om militär underrättelseverksamhet och som har samband med den här propositionen behandlas på motsvarande sätt lagstiftningen i Sverige, Nederländerna och Schweiz. De delar av propositionen där jämförelseländernas lagstiftning presenteras har utarbetats av inrikesministeriet och försvarsministeriet tillsammans. I denna proposition hänvisas det till skillnad från försvarsministeriets proposition till den internationella jämförelse som försvarsministeriet tagit fram om Sverige, Nederländerna och Schweiz. Det bör påpekas att den rättsliga övervakningen och parlamentariska tillsynen av underrättelseinhämtningen i jämförelsestaterna behandlas i den proposition av justitieministeriet som anknyter till denna proposition och som gäller lagstiftning om övervakning av underrättelseverksamhet.

Till den internationella jämförelsen valdes Sverige, Norge, Danmark och Tyskland samt Nederländerna och Schweiz. Valet av de nordiska länderna är självklart till följd av likheterna när det gäller rättssystem och rättskultur. Också det tyska rättssystemet ligger nära vårt nationella system. Mer specifikt har lagstiftningen i Tyskland i Europadomstolens avgöranden inom ämnesområdet ansetts ligga i linje med Europakonventionen.

Beredningen av lagstiftningen om underrättelseinhämtning har följt jämförelseländernas lagstiftning sedan 2013. Propositionens beskrivning av hur underrättelseverksamheten är organiserad är tillräckligt detaljerad. Känsliga frågor är kopplade till organiseringen av den operativa underrättelseverksamheten och därför är det inte möjligt att beskriva den närmare i propositionen.

Både Schweiz och Nederländerna började se över sin lagstiftning om underrättelseinhämtning när denna proposition bereddes. Båda länderna är väl förankrade europeiska rättsstater och därför lämpade sig välfungerande förfaranden inom de lagstiftningsprojekten bra som jämförelsematerial för denna proposition. Också den pågående reformeringen av lagstiftningen om underrättelseinhämtning i Norge följdes noggrant.

Propositionen innehåller inga tabeller över läget i fråga om den aktuella lagstiftningen i olika länder. Det beror på att länderna valt olika lagstiftningslösningar som till exempel i fråga om avgränsningens exakthet avviker märkbart från varandra och en jämförelse skulle då inte ge något mervärde för konsekvensbedömningen. Dessutom har det ansetts att tabeller de facto inte skulle kasta ljus över frågan.

Det är fråga om helt ny lagstiftning och ett sådant komplex att konsekvensbedömningen accentuerar förhandsbedömning och dessutom särskilt analys i efterskott. Därför kan man för riksdagen föreslå att den överväger att uppställa en skyldighet att följa hur lagstiftningen verkställs och genomförs. Perioden för detta bör vara tillräckligt lång för att analysen i efterskott kan göras utifrån ett tillräckligt material. När mätkriterierna för uppföljningen bestäms är det dock viktigt att de bildar en helhet som kan ge så omfattande och objektiv information som möjligt för behövliga slutsatser. De utrikespolitiskt eller annars känsliga frågor som är kopplade till underrättelseverksamhet sätter vissa gränser när kriterierna ska bestämmas.

6 Samband med andra propositioner

Vid försvarsministeriet pågår ett lagstiftningsprojekt där man föreslår att det stiftas en lag om militär underrättelseinhämtning. Den propositionen överlämnas samtidigt som denna proposition. Regeringens proposition som gäller militär underrättelseinhämtning och denna proposition hör samman särskilt när det gäller regleringen om och i anslutning till metoder för underrättelseinhämtning.

Vid justitieministeriet har man berett ett förslag om ändring av grundlagen som gäller begränsningar i skyddet för förtroliga meddelanden för att skydda den nationella säkerheten i syfte att inhämta information om militär verksamhet och annan verksamhet som hotar den nationella säkerheten. När denna ändring genomförs i grundlagen blir det möjligt att i lagstiftningen om civil och militär underrättelseinhämtning föreskriva om nödvändiga metoder för underrättelseinhämtning som saknas i skyddet för hemligheten i fråga om förtroliga meddelanden.

Vid justitieministeriet har förutom det ovannämnda förslaget beretts ett förslag om övervakning av underrättelseverksamhet som hänför sig till denna proposition. I denna proposition föreskrivs i 5 a kap. 60 § i polislagen om extern övervakning av den civila underrättelseinhämtningen och i 61 § om anmälningar till underrättelseombudsmannen samt i 25 § i det lagförslag

som gäller civil underrättelseinhämtning avseende datatrafik om extern övervakning av underrättelseinhämtning som avser datatrafik och i 26 § om anmälningar till underrättelseombudsmannen. I lagförslaget om övervakning av underrättelseverksamheten föreskrivs åter om rätt för underrättelseombudsmannen att närvara vid domstolsförfarande som avses i 5 a kap. 35 § i förslaget som gäller polislagen.

Inrikesministeriet har den 28 januari 2016 tillsatt ett projekt i syfte att reformera lagstiftningen om behandling av personuppgifter i polisens verksamhet. Avsikten är att regeringens proposition med förslag till en totalreform av lagen om behandling av personuppgifter i polisens verksamhet ska överlämnas under vårsessionen 2018. Eftersom de nya underrättelsebefogenheterna vid sidan av andra uppgifter ger även personuppgifter, och eftersom regleringen om underrättelsebefogenheter eventuellt träder i kraft före den reviderade lagen om behandling av personuppgifter i polisens verksamhet, föreslås i denna proposition att den sistnämnda lagen ändras.

DETALJMOTIVERING

1 Lagförslag

1.1 Polislagen

1 kap. **Allmänna bestämmelser**

1 §. *Polisens uppgifter.* Enligt förslaget ska 1 mom. ändras genom ett tillägg som anger att det också hör till polisens uppgifter att skydda den nationella säkerheten. Polisens uppgift är således enligt första meningen i det momentet att trygga rätts- och samhällsordningen, skydda den nationella säkerheten, upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning.

Begreppet nationell säkerhet förekommer i många internationella avtalshandlingar. Enligt artikel 8 i Europakonventionen är statens säkerhet en av de grunder som ger rätt till inskränkning av skyddet för privatlivet. Staten har en relativt omfattande prövningsmarginal i fråga om vilken verksamhet de anser hota den nationella säkerheten. Även enligt artikel 4.2 i fördraget om Europeiska unionen ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar, även om detta inte är helt entydigt.

Begreppet nationell säkerhet har ett brett innehåll som delvis saknar struktur, och dess betydelseinnehåll har inte preciserats i någon nämnvärd utsträckning i överstatliga avtal. Nationell säkerhet kan åtminstone anses innebära det att verksamhet som hotar den säkerheten primärt inte riktar sig mot någon som individ utan mer allmänt mot staten eller samhället. Betydelseinnehållet förändras och formas i takt med samhälleliga och även globala förändringar. Bland annat därför används begreppet nationell säkerhet, och dess närmare innehåll kommer att definieras utifrån verksamhet som hotar den säkerheten. Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen) har i sin avgörandepraxis ansett att åtminstone militärt försvar, bekämpning av terrorism och bekämpning av olaglig underrättelseverksamhet omfattas av den nationella säkerheten (bl.a. Klass mot Tyskland, Weber och Saravia mot Tyskland). Frågan behandlas närmare i den del av den allmänna motiveringen som gäller de internationella aspekterna.

Det är således fråga om ett slags kollektivt skyddsintresse när vi talar om nationell säkerhet, och detta intresse får sitt innehåll av den enskilda medborgarens grundläggande fri- och rättigheter. Samtidigt kan ett våldsdåd som riktas mot en enskild person på grund av hans eller hennes ämbete eller ställning vara sådan verksamhet som avses i bestämmelsen, om avsikten är att påverka staten eller samhället. Det kan vara fråga om en sådan situation exempelvis om hotet riktar sig mot den högsta statsledningen. Dessutom kan agerande som till exempel hotar personer som deltar i internationella krishanterings- eller biståndsuppdrag vara här avsedd verksamhet. Deltagande i sådana uppdrag ingår i Finlands utrikes- och säkerhetspolitik.

I och med den ökande internationaliseringen har gränsen mellan statens yttre och inre säkerhet blivit allt mer vacklande. Det är också allt svårare att göra en territorie- eller platsbunden avgränsning av hot och risker när de ekonomiska, tekniska och sociala systemen blir allt mer gränsöverskridande och inbördes beroende av varandra.

Verksamhet som hotar den nationella säkerheten kan grovt taget indelas i verksamhet av civil natur och verksamhet av militär natur. Det är emellertid inte möjligt att göra någon exakt indelning eftersom både militära hot och hotfull verksamhet av civil natur kan utgöra ett hot eller allvarligt hot mot den nationella säkerheten. Indelningen av sådan verksamhet handlar mer om ändamålsenlighet när det gäller uppgiftsfördelningen mellan myndigheterna för civil re-

spektive militär underrättelseverksamhet. Till de viktigaste säkerhetshoten av civil natur hör åtminstone terrorism, spioneri mot Finland och dess intressen från främmande makts sida, försök att sprida massförstörelsevapen och produkter med dubbla användningsområden och sådan internationell organiserad brottslighet vars syfte är att påverka det samhälleliga beslutsfattandet eller infiltrera de statliga strukturerna. Under de senaste åren har särskilt gränsöverskridande spioneri i datanät vuxit fram som ett betydande hot. Sådan verksamhet gör det möjligt att skaffa stora datamängder på en gång, vilket kan leda till irreparabel skada för den utsatta statens säkerhet och dess intressen. Närmare bestämmelser om verksamhet som allvarligt hotar den nationella säkerheten finns i 5 a kap. 3 §.

Det är det allmänna som ska skydda den nationella säkerheten. I många länder har man koncentrerat uppgiften att skaffa upplysningar om verksamhet som hotar eller allvarligt hotar den nationella säkerheten genom befogenheter till underrättelseinhämtning till vissa underrättelsemyndigheter. Skyddspolisen har numera till uppgift att bland annat bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet samt att utföra undersökning av sådana brott. När skyddspolisen ska förhindra och avslöja brott inom sitt uppgiftsområde krävs det så tidig inhämtning av information som bara är möjlig med hemliga metoder för informationsinhämtning till följd av brott. Detta kan motiveras bland annat med att den skada som uppkommer när rekvisitet för sådana brott uppfylls kan vara mycket kännbar för exempelvis Finlands yttre förbindelser, statsfinanser, utrikeshandel, energiförsörjning eller säkerhet. Därför är det främst i skyddspolisens verksamhet som det kan bli fråga om att också använda metoder för underrättelseinhämtning inom den civila underrättelseinhämtningen. Detta framgår också av det föreslagna nya 5 a kap. i polislagen och av det föreslagna nya 10 § 1 mom. i polisförvaltningslagen, där det sägs att skyddspolisen har till uppgift att i enlighet med inrikesministeriets styrning inhämta information för att skydda den nationella säkerheten samt upptäcka, förhindra och avslöja sådan verksamhet, sådana förehavanden och sådana brott som kan hota stats- och samhällsordningen eller rikets inre eller yttre säkerhet. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att upptäcka och förhindra verksamhet som hotar samhällets säkerhet.

Bestämmelsen om polisen uppgifter i 1 kap. 1 § i polislagen är inte behörighetsgrundande, vilket innebär att polisen inte enbart med stöd av den får ingripa i människors lagfästa rättigheter. När polisen ingriper i individens rättssfär ska befogenheten alltid grunda sig på en uttrycklig bestämmelse. Med andra ord är skyddet av nationell säkerhet i sig bara ett uttryck för att skyddspolisen har ett lagenligt och från samhällets sida accepterat motiv för sitt förfarande. Detta ger således inte i sig rätt att ingripa i människors grundläggande fri- och rättigheter. För det krävs det en lagfäst behörighetsgrund.

5 kap. **Hemliga metoder för inhämtande av information**

5 §. *Teleavlyssning och dess förutsättningar*. I första meningen i 1 mom. föreslås ändring av definitionen av teleavlyssning eftersom definitionen i den gällande lagen hänvisar till den upphävda kommunikationsmarknadslagen.

Enligt den föreslagna definitionen avser teleavlyssning att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett sådant allmänt kommunikationsnät eller ett sådant därtill anslutet kommunikationsnät som avses i 3 § 43 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 8 §. Teleavlyssning ska få riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas göra sig skyldig till ett brott som avses i 2 mom.

Avsikten är inte att i sak ändra definitionen av teleavlyssning eller definitionens tillämpningsområde, utan ändringen är rent teknisk.

7 §. *Beslut om teleavlyssning och motsvarande inhämtande av information.* Enligt förslaget ska 1 mom. ändras så att domstolen ska besluta om teleavlyssning och inhämtande av information i stället för teleavlyssning på yrkande av en polisman som avses i 2 kap. 9 § 1 mom. 1 punkten i tvångsmedelslagen (anhållningsberättigad polisman) eller chefen eller biträdande chefer för skyddspolisen eller avdelningschefer, överinspektörer eller inspektörer vid skyddspolisen (polisman som hör till befälet vid skyddspolisen). Dessutom ändras 3 mom. 6 punkten så att den syftar till polismän som avses i 1 mom.

Enligt rapporten från en arbetsgrupp som utredde skyddspolisens administrativa ställning, resultatstyrningen och utveckling av övervakningen bör man överväga begränsning av skyddspolisens förundersökningsuppgifter och inskränkning eller slopande av dess förundersökningsbefogenheter, om dess underrättelsebefogenheter utvidgas. Denna fråga behandlas närmare i den allmänna motiveringen och i detaljmotiveringen till förslagen till lag om ändring av förundersökningslagen respektive tvångsmedelslagen.

Slopad förundersökningsbehörighet skulle också innebära att tvångsmedelsbefogenheterna inskränks eller slopas, och då skulle skyddspolisen inte längre ha vare sig anhållningsberättigade tjänstemän eller anhållningsberättigade polismän. De polismän som hör till befälet inom skyddspolisen bör i så fall börja kallas ”polisman som hör till befälet vid skyddspolisen”, med vilket man avser chefen eller biträdande chefer för skyddspolisen eller avdelningschefer, överinspektörer eller inspektörer vid skyddspolisen.

8 §. *Teleövervakning och dess förutsättningar.* I 1 mom. föreslås en precisering av definitionen av teleövervakning eftersom den gällande lagen hänvisar till den upphävda lagen om dataskydd vid elektronisk kommunikation och genom en kedja av hänvisningar till kommunikationsmarknadslagen, som nämns i den bestämmelse där teleavlyssning definieras (5 kap. 5 §). Också den lagen har upphävts.

Enligt den föreslagna definitionen avses med teleövervakning att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät som avses i 5 § eller som har mottagits till en sådan adress eller utrustning samt att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att användningen av adressen eller utrustningen tillfälligt förhindras. Med identifieringsuppgifter ska avses sådana uppgifter om ett meddelande som kan förknippas med en användare som avses i 3 § 7 punkten i lagen om tjänster inom elektronisk kommunikation eller med en sådan abonnent som avses i 30 punkten i den paragrafen och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.

Avsikten är inte att i sak ändra definitionen av teleövervakning eller definitionens tillämpningsområde, utan ändringen är rent teknisk.

10 §. *Beslut om teleövervakning.* Enligt förslaget ska polismän som hör till befälet vid skyddspolisen enligt det föreslagna 7 § 1 mom. fogas till som beslutsfattare i 10 § 1—4 och 6 mom.

12 §. *Beslut om inhämtande av basstationsuppgifter.* Polismän som hör till befälet vid skyddspolisen läggs till som beslutsfattare i 1 mom. Vidare ändras 3 mom. 5 punkten så att man i fråga om den polisman som beslutar om inhämtandet av information hänvisar till 7 § 1 mom., varvid yrkandet och beslutet måste nämna den polisman som leder och övervakar inhämtandet

av basstationsuppgifter och som avses i 7 § 1 mom. I detta avseende är det som framförs i motiveringen till 7 § relevant.

14 §. *Beslut om systematisk observation.* I fråga om motiveringen hänvisas det till vad som framförs i motiveringen till 12 §.

16 §. *Beslut om förtäckt inhämtande av information.* Det föreslås att 1 mom. ändras så att polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggs till som beslutsfattare. En här avsedd polisman ska ha utbildats särskilt för hemligt inhämtande av information.

18 §. *Beslut om teknisk avlyssning.* Ändring av 2 mom. föreslås. Enligt förslaget ska polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare i 18 § 2 mom. Vidare ändras 4 mom. 6 punkten så att den avser den polisman som leder och övervakar genomförandet av den tekniska avlyssningen och som avses i 7 § 1 mom.

20 §. *Beslut om optisk observation.* Det föreslås att 1, 2 och 4 mom. ändras så att polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggs till som beslutsfattare.

22 §. *Beslut om teknisk spårning.* Det föreslås att 1, 2 och 4 mom. ändras så att polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggs till som beslutsfattare.

24 §. *Beslut om teknisk observation av utrustning.* Det föreslås att 1 och 3 mom. ändras så att polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggs till som beslutsfattare.

25 §. *Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning.* I 3 mom. ska enligt förslaget polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare. En här avsedd polisman ska ha utbildats särskilt för hemligt inhämtande av information.

32 §. *Beslut om en täckoperation.* I 1 mom. ska enligt förslaget polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare.

36 §. *Beslut om bevisprovokation genom köp.* Det föreslås att 1 och 3 mom. ändras så att polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggs till som beslutsfattare. En här avsedd polisman ska ha utbildats särskilt för hemligt inhämtande av information.

38 §. *Beslut om genomförande av bevisprovokation genom köp.* I 1 mom. ska enligt förslaget polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare. En här avsedd polisman ska ha utbildats särskilt för hemligt inhämtande av information.

39 §. *Säkerheten för en polisman vid förtäckt inhämtande av information, en täckoperation och vid bevisprovokation genom köp.* I 1 mom. ska enligt förslaget polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare.

40 §. *Användning av informationskällor och förutsättningar för styrd användning av informationskällor.* Enligt paragrafen ska med användning av informationskällor avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av i 1 kap. 1 § av-

sedda uppgifter av personer som inte hör till polisen eller till någon annan myndighet (informationskälla).

Enligt den gällande lagen kan endast personer som inte hör till polisen eller till någon annan förundersökningsmyndighet vara informationskällor. I praktiken har det förekommit oklarheter i fråga om huruvida en tjänsteman vid en annan myndighet än en förundersökningsmyndighet ska registreras som informationskälla. Därför föreslås den nämnda preciseringen, och då är det personer som inte hör till en polisiär myndighet eller till någon annan myndighet som är informationskällor.

42 §. *Beslut om styrd användning av informationskällor.* I 1 mom. ska enligt förslaget polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare. En här avsedd polisman ska ha utbildats särskilt för hemligt inhämtande av information.

44 §. *Beslut om kontrollerade leveranser.* I 1 mom. ska enligt förslaget polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare. En här avsedd polisman ska ha utbildats särskilt för hemligt inhämtande av information.

47 §. *Beslut om skyddande.* I 2 mom. ska enligt förslaget polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare. En här avsedd polisman ska ha utbildats särskilt för hemligt inhämtande av information.

48 §. *Yppandeförbud som gäller hemligt inhämtande av information.* Förslaget innebär att polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggs till som beslutsfattare i 48 § 1 mom.

52 §. *Undersökning av upptagningar.* Förslaget innebär att polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggs till som beslutsfattare i 52 §.

57 §. *Utplåning av information som fåtts i en brådskande situation.* Förslaget innebär att också polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. nämns i 57 §.

58 §. *Underrättelse om hemligt inhämtande av information.* Det föreslås att systematisk observation och förtäckt inhämtande av information utgår ur 1 mom. Det beror på första meningen i 5 mom. i samma paragraf . Enligt den behöver den som varit föremål för inhämtande av information inte underrättas om systematisk observation och förtäckt inhämtande av information, om inte förundersökning har inletts i ärendet. Enligt andra meningen i samma moment ska bestämmelserna i 10 kap. 60 § i tvångsmedelslagen iakttas i tillämpliga delar, om förundersökning inleds.

Avsikten är att slopa den oklarhet i tolkningen mellan 1 och 5 mom. som framkommit i den konkreta verksamheten.

61 §. *Teleföretags skyldighet att biträda samt tillträde till vissa utrymmen.* I 2 mom. ska enligt förslaget polismän som hör till befälet vid skyddspolisen enligt definitionen i 7 § 1 mom. läggas till som beslutsfattare.

63 §. *Tillsyn över hemligt inhämtande av information.* I 2 mom. föreslås en teknisk justering i den finska lagtexten, dvs. den finska benämningen på inrikesministeriet, ”sisäasiainministeriö”, ändras till ”sisäministeriö”.

5 a kap. **Civil underrättelseinhämtning**

1 §. *Tillämpningsområde.* Paragrafen avses innehålla definitionen av civil underrättelseinhämtning och bestämmelser om tillämpningsområdet. Med civil underrättelseinhämtning avses skyddspolisens inhämtande och nyttjande av information för att den nationella säkerheten ska kunna skyddas och den högsta statsledningens beslutsfattande stödjas samt för att andra myndigheter ska kunna utföra sina lagstadgade uppgifter som hänför sig till den nationella säkerheten (*civil underrättelseinhämtning*).

Syftet är att framhäva att skyddspolisen avses vara den enda myndigheten med rätt att använda de metoder för underrättelseinhämtning som avses i kapitlet och att med de befogenheterna inhämta information om verksamhet som hotar den nationella säkerheten. Genom civil underrättelseinhämtning och metoderna för underrättelseinhämtning ger man skyddspolisen möjlighet att tillräckligt effektivt inhämta information om de fenomen och planer som utgör de allvarligaste hoten mot samhället.

Skyddet av den nationella säkerheten ska i sig som begrepp vara mer omfattande än den verksamhet som får skyddspolisen att tillgripa metoder för underrättelseinhämtning och som potentiellt utgör ett hot mot den nationella säkerheten. Att skydda nationell säkerhet ska innefatta dels utövande av skyddspolisens befogenheter, dels också tillräckligt effektivt nyttjande av den information som inhämtats med stöd av befogenheterna. Med detta avses åtminstone att man sörjer för att den högsta statsledningens beslutsfattande bygger på korrekt, aktuell och tillförlitlig information och att man gör det möjligt för andra behöriga myndigheter att börja avvärja hot.

Samtidigt ska det också kunna anses att en tillräckligt effektiv övervakning av underrättelseverksamheten utgör skydd av nationell säkerhet; syftet är då att se till att underrättelseverksamheten inte upphör att fylla sitt syfte eller blir ineffektiv. Europadomstolen har i sin avgörandepraxis understrukit vikten av att myndigheternas hemliga observationsbefogenheter övervakas och att övervakningen ska ordnas effektivt. Dessutom får man inte heller låta övervakningen bli helt beroende av myndighetens interna kontroll.

I definitionen av civil underrättelseinhämtning nämns uttryckligen den högsta statsledningen och andra myndigheter för nationell säkerhet. Avsikten är då att understryka ändamålsbundenheten i den inhämtning av information som skyddspolisen utför i anknytning till sitt uppdrag. Syftet med civil underrättelseinhämtning avses därmed vara att genom skyddspolisens informationsinhämtning skydda den nationella säkerheten antingen genom att själv använda informationen eller genom att dela informationen med andra relevanta myndigheter som har uppgifter inom skyddet av nationell säkerhet eller anknytande uppgifter. Dessutom ingår det redan nu i skyddspolisens uppgifter att leverera analyserade data till den högsta statsledningen. Nu ska denna uppgift dock uttryckligen nämnas i lag. Utöver i syfte att skydda nationell säkerhet ska skyddspolisen inte få utöva sina befogenheter för andra syften än de som uttryckligen hänför sig till uppgiften. Senare i lagförslaget ingår också bestämmelser om undantag från ändamålsbundenheten (44 §).

2 §. *Metoder för civil underrättelseinhämtning.* Paragrafen avses innehålla bestämmelser om metoderna för underrättelseinhämtning, dvs. om de befogenheter till underrättelseinhämtning som polisen får utöva för civil underrättelseinhämtning.

Att tillämpa metoder för underrättelseinhämtning med avseende på personer eller grupper av personer utgör utan undantag att man inkräktar i den eller de berörda personernas integritetsskydd. Utgångspunkten är att metoderna för underrättelseinhämtning används utan att objektet vet om det. Underrättelseverksamheten och underrättelseinhämtningsmetoderna är till sin na-

tur fördolda och användningen av en sådan metod och den information detta ger, ger därför inte i sig upphov till samma typ av skada eller negativa effekter som exempelvis flera tvångsmedel (anhållande, häktning eller kvarstad) gör. Den inhämtade informationen används heller inte a priori som bevis för att den berörda personen är skyldig, och dessutom ingriper man inte genom den i den berörda personens integritet eller frihet på samma sätt som genom tvångsmedel. Däremot gör man det möjligt att med relativt låg tröskel använda den inhämtade informationen som stöd för att bevisa att någon inte är skyldig.

Det finns skäl att särskilt ge akt på att de grundläggande och mänskliga rättigheterna respekteras när metoder för underrättelseinhämtning används. Metoderna inkräktar a priori i de grundlagsfästa grundläggande fri- och rättigheterna. Detta gäller i synnerhet skyddet för privatlivet och i fråga om förtroliga meddelanden. Skyddet för grundläggande och mänskliga rättigheter måste emellertid samtidigt vägas mot intresset att skydda den nationella säkerheten. Dessa motsatta intressen utesluter i och för sig inte varandra, eftersom vars och ens grundläggande fri- och rättigheter och mänskliga rättigheter skyddas samtidigt när den nationella säkerheten skyddas och för samhället skadliga händelser förhindras. Metoderna för underrättelseinhämtning får heller inte användas på ett diskriminerande sätt och inte heller utifrån etnisk profilering eller på ett sätt där man inhämtar information om någon uteslutande eller huvudsakligen på grundval av personens etniska bakgrund, hudfärg eller religion.

Också andra polisrättsliga principer, proportionalitetsprincipen, principen om minsta olägenhet och principen om ändamålsbundenhet, ska beaktas särskilt när metoderna används. Proportionalitetsprincipen kommer att kräva att man alltid ska bedöma åtgärdernas skälighet, vilket innebär att de metoder som man väljer att använda och den olägenhet detta medför, exempelvis ingrepp i integritetsskyddet, alltid ska stå i rimlig proportion till det eftersträvande målet. Skälighet eller proportionalitet innebär således inte att åtgärden inte får vara överdimensionerade ur den utsattes synvinkel, utan det är också fråga om att åtgärden måste vara tillräckligt effektiv för att det eftersträvade målet, exempelvis erhållande av viss information, ska kunna nås. Proportionalitetsprincipen framgår dels av det som står i 1 kap. 3 §, dels också av den rättighet som anges i 9 § 1 mom. i samma kapitel och som gäller rätten att avstå från en åtgärd, om dess slutförande kan leda till ett oskäligt resultat i förhållande till det eftersträvade målet.

Principen om minsta olägenhet framgår av 1 kap. 4 §, där det står att det inte får ingripas i någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenhet än vad som är nödvändigt för att utföra uppdraget. Med rättigheter avses då de grundlagsfästa fri- och rättigheterna. Principen om minsta olägenhet förpliktar skyddspolisen att ingripa så lite som möjligt i den personens grundläggande fri- och rättigheter som är föremål för metoderna för underrättelseinhämtning. Med ”ingen” menas att principen om minsta olägenhet skyddar alla som påverkas av polisens åtgärd. Det framgår väl av principen att ett nödvändighetsvillkor och en därav följande optimeringsskyldighet i fråga om (i detta sammanhang) alternativa metoder för underrättelseinhämtning hör till dess byggstenar. Dessa element styr skyddspolisens verksamhet inom civila underrättelseinhämtning och när metoden för underrättelseinhämtning och dess objekt ska väljas. När den civila underrättelseinhämtningen inleds och den valda metoden börjar användas ska verksamheten genomföras på ett sätt som inkräktar så lite som möjligt på det valda objektets grundläggande fri- och rättigheter. Med detta avses en skyldighet att minimera den skada eller olägenhet som objektet utsätts för.

Bestämmelser om principen om ändamålsbundenhet finns i 1 kap. 5 §, där det sägs att polisen får utöva sina befogenheter endast i föreskrivna syften. Principen anknyter i detta sammanhang både till ändringarna i 10 § i polisförvaltningslagen och till ändringarna i 1 kap. 1 § i polislagen samt till det som i motiveringen till ändringarna sägs om att polisens befogenheter alltid ska bygga på en uttrycklig bestämmelse. Om ingreppet gäller en individs rättigheter eller

skyldigheter måste den bestämmelsen finnas i lag. Principen om ändamålsbundenhet gäller alla polisiära åtgärder och i detta sammanhang är den relevant med avseende på utövandet av befogenheterna till civil underrättelseinhämtning, särskilt den information som inhämtats med stöd av dem.

I 1 mom. räknas de metoder för underrättelseinhämtning upp som definitionsmässigt huvudsakligen motsvarar i 5 kap. nämnda hemliga metoder för inhämtande av information och i fråga om vilka villkoren för användning anges närmare i detta kapitel. Eftersom definitioner av de hemliga metoderna redan finns i 5 kap. behövs ingen upprepning av definitionerna i 5 a kap. Därför är det meningen att i 5 a kap. bara föreskriva om villkoren för att befogenheterna ska få utövas och om beslutsprocessen när metoder för underrättelseinhämtning ska användas.

Metoderna avses innefatta följande metoder enligt 5 kap.: teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, teknisk spårning, teknisk observation av utrustning, inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp och styrd användning av informationskällor. Kontrollerade leveranser nämns inte i förteckningen och de räknas inte till metoderna för underrättelseinhämtning. Befogenheten i fråga lämpar sig inte för användning som befogenhet för underrättelseinhämtning, eftersom det utifrån innehav eller transport av föremål, ämnen eller egendom som är föremål för kontrollerade leveranser finns anledning att misstänka brott eller grundad anledning att misstänka att någon gör sig skyldig till brott. I sådana fall ska man i regel vid hemligt inhämtande av information använda brottsbaserade fullmakter för sådant inhämtande.

Momentet nämner heller inte deltagande i en organiserad kriminell sammanslutnings verksamhet och i kontrollerade leveranser. Inom den civila underrättelseinhämtningen bör den befogenheten uteslutas eftersom dess tillämpning inom den inte kan komma på fråga. Deltagande i en organiserad kriminell sammanslutnings verksamhet och i kontrollerade leveranser anknyter till täckoperationer på grundval av brott. I praktiken är det ändå inte möjligt att göra någon väldigt tydlig skillnad mellan sådana grupper vars verksamhet allvarligt hotar den nationella säkerheten och sådana gruppen som begår brott.

Brottsförbud ska däremot tillämpas inom civil underrättelseinhämtning, eftersom grunden för och syftet med täckoperationer inte är att skaffa information om att de som är föremål för underrättelseinhämtningen gjort sig skyldiga till de förseelser som avses i paragrafen om brottsförbud. Det är fråga om att personer som deltar i täckoperationer med nödvändighet måste kunna begå sådana förseelser för att förhindra att operationen avslöjas. Intresset att undvika att bli avslöjad är därmed inte kopplat till frågan om täckoperationen utförs för att bekämpa brott eller för civil underrättelseinhämtning.

Enligt 2 mom. ska metoderna för underrättelseinhämtning också inbegripa de helt nya befogenheterna enligt kapitlet, dvs. platsspecifik underrättelseinhämtning, kopiering, kvarhållande av en försändelse för kopiering och inhämtande av information från privata sammanslutningar. Dessa befogenheter har ingen motsvarighet i 5 kap., vilket kräver att de definieras som metoder för underrättelseinhämtning i ett separat moment.

Enligt 3 mom. ska detta kapitel ange under vilka förutsättningar de metoder som anges i 1 mom. samt platsspecifik underrättelseinhämtning, kopiering, kvarhållande av en försändelse för kopiering och rätt att få information av privata sammanslutningar får användas inom civil underrättelseinhämtning.

Med förutsättningar avses då uttryckligen förutsättningarna enligt detta kapitel och uttrycket ”förutsättningarna för” utesluter därmed förutsättningarna för användning av de hemliga metoderna för inhämtande av information enligt 5 kap. Det behövs sådan reglering eftersom definitionerna av de metoder för underrättelseinhämtning som nämns i 1 mom. återfinns i 5 kap. och förutsättningarna för användning och bestämmelserna om beslutsfattande i detta kapitel.

Det är meningen att metoderna för underrättelseinhämtning ska användas för att skaffa information om verksamhet som inte är kopplad till brottsmisstanke. Om det av definitionsbestämmelsen (5 kap.) till någon av de befogenheter som avses i detta moment framträder ett brottselement ska den bestämmelsen inte tillämpas när metoderna för underrättelseinhämtning i 5 a kap. används, eftersom metoden inte används för att skaffa information för att förhindra, avslöja eller utreda brott. Dessutom avser ”förutsättningarna för” också hur utövandet av befogenheten inriktas. Det går heller inte att använda metoderna så att de alltid gäller en viss person; det ligger i underrättelseverksamhetens natur. Också en grupp av personer kan komma i fråga.

Exempelvis föreskrivs följande om systematisk observation i 5 kap. 13 § 2 mom.: Med systematisk observation avses annan än kortvarig observation av en person som med fog kan antas göra sig skyldig till ett brott. Med brottselement avses relativsatsen i slutet av definitionen. Villkoren för användning av sådan observation som metod för underrättelseinhämtning avses framgå av 5 a kap. 4 och 9 §. Ett villkor för att systematisk observation ska få användas är att man med fog kan vänta sig att den ger information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som hotar den nationella säkerheten. Föremålen för civil underrättelseinhämtning räknas upp i en uttömmande förteckning i 3 §. Ett villkor för att systematisk observation ska få användas är också att den med fog kan antas ha mycket stor betydelse när det gäller att få information om den verksamhet som är föremål för civil underrättelseinhämtning och som hotar den nationella säkerheten. Beslut om systematisk observation får enligt 9 § 2 mom. fattas för högst sex månader åt gången. Objektet för systematisk observation vid civil underrättelseinhämtning kan på det sätt som framgår av 9 § 3 mom. också vara en grupp av personer.

Såsom redan sagts ovan ska användningen av metoderna för underrättelseinhämtning inte vara knuten till brott på det sätt som anges i 5 kap. Villkoren för användningen anges i 5 a kap. med avseende på skyddet för nationell säkerhet. Med detta menar man framför allt att intresset att inhämta information gäller verksamhet som hotar eller allvarligt hotar den nationella säkerheten, inte ett misstänkt eller antaget brott och de delaktiga. Dessutom anges de konkreta objekten för användning av metoder för underrättelseinhämtning (t.ex. personer, grupper, utrymmen eller någon annan plats) nedan särskilt för varje metod.

Utöver villkoren för användning innehåller 5 a kap. också bestämmelserna om beslutsfattande i fråga om metoderna. Enligt dem ska den verksamhet som användningen av metoderna gäller i varje enskilt fall specificeras och motiveras. Det ska för användning av metoderna inte krävas att den som ligger bakom hotfull verksamhet ska ha identifierats vid den tidpunkt då en metod för underrättelseinhämtning börjar användas. Med detta avses att metoderna också får användas för att upptäcka hot och identifiera dem som ligger bakom hotet. Därmed kan en sådan person eller grupp vara objekt för underrättelseinhämtning som kan antas besitta information om verksamhet som hotar den nationella säkerheten. Underrättelseinhämtningen ska kunna inriktas mot såväl statliga som icke-statliga aktörer och mot sådana personer som agerar på en statlig aktör vägnar eller till dennes förmån.

I 4 mom. nämns lagen om civil underrättelseinhämtning avseende datatrafik. Civil underrättelseinhämtning som avser datatrafik ska också vara en metod för underrättelseinhämtning och en befogenhet som skyddspolisen har för civil underrättelseinhämtning. Befogenheten får ut-

övas för att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten.

3 §. *Föremål för civil underrättelseinhämtning.* Paragrafen avses innehålla bestämmelser om föremålen för civil underrättelseinhämtning. Det ska vara tillåtet att inhämta information om dem med de metoder för underrättelseinhämtning som avses i kapitlet. Förteckningen avses vara uttömmande. I 3 § i lagen om civil underrättelseinhämtning avseende datatrafik föreslås en bestämmelse med samma innehåll om verksamhet som allvarligt hotar den nationella säkerheten.

Enligt 1 punkten får metoderna användas för att inhämta information om terrorism.

Terrorism definieras allmänt som handlingar som begås i syfte att injaga allvarlig fruktan hos en befolkning, otillbörligen tvinga offentliga organ eller en internationell organisation att utföra eller att avstå från att utföra en viss handling eller allvarligt destabilisera eller förstöra de grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturerna i ett land eller i en internationell organisation (se t.ex. FN:s säkerhetsråds resolution 1566 (2004) och Europeiska unionens råds rambeslut 2002/475/RIF). Metoderna för underrättelseinhämtning ska få användas för att inhämta information om terrorism som fenomen eller om konkreta planer.

Information kan inhämtas om exempelvis fenomenet utländska stridande (om begreppet utländsk stridande, se FN:s säkerhetsråds resolution 2178 (2014)) eller om stödjande av sådan verksamhet eller så om hurdana planer eller ändamål eller hurdan förmåga att genomföra en attack ledningen för en terroristorganisation har i fråga om Finland, och vidare vilka personer som har kopplingar till en sådan organisations verksamhet och hur dessa styrs från utlandet. Metoderna för underrättelseinhämtning ska också kunna användas för att inhämta information om terrorismrelaterad våldsinriktad radikalisering. Information som inhämtas i tillräckligt god tid kan utgöra ett stöd när det gäller att förhindra terroristattacker mot Finland eller mot någon främmande stat från Finland och att förebygga spridning av terroristisk verksamhet i eller från Finland. Enligt 2 punkten får metoderna användas för att inhämta information om utländsk underrättelseverksamhet.

Med främmande staters underrättelseinhämtning avses verksamhet där information inhämtas i syfte att främja den egna statens intressen eller att skada Finlands eller någon annan främmande stats intressen och där målstaten har ett särskilt intresse att hålla den information som inhämtas hemlig. Den information som den främmande staten försöker skaffa sig kan gälla till exempel Finlands utrikespolitik, säkerhetspolitik eller energipolitik, Finlands militära beredskap, samhällets kristålighet, försörjningsberedskapen och högteknik med tillhörande forskning och produktutveckling. Främmande stater vill inte bara inhämta information, utan deras underrättelseverksamhet siktar också bland annat på att påverka beslutsfattandet när det gäller de nämnda sakerna, och syftet är då att främja deras egna intressen eller att skada Finlands eller någon annan främmande stats intressen.

Metoderna för underrättelseinhämtning kan användas till exempel för att skaffa information om hur en främmande stats underrättelseinhämtning fungerar, vem som handlar för den utländska underrättelsetjänstens räkning eller till dess förmån eller vilka deras öppna eller hemliga metoder och objekt för underrättelseinhämtning är. Information kan också inhämtas exempelvis om vilka mål och prioriteringar främmande stater har för den information som deras underrättelsetjänst ska inhämta om Finland. Metoderna kan också användas till att upptäcka och identifiera personer som avslöjar sekretessbelagd information för främmande staters underrättelsetjänst, som främmande staters underrättelsetjänster försöker värva för sådan verksamhet eller som i enlighet med order eller instruktioner från sådana staters underrättelsetjänst försöker påverka beslutsfattandet till skada för Finland eller en annan främmande stat. Vidare

kan information också inhämtas om sådan mot företag riktad underrättelseinhämtning vars syfte är att lyckas överlämna företagens kunskapskapital till en främmande stat.

Enligt 3 punkten får metoderna användas för att inhämta information om massförstörelsevapen.

Med massförstörelsevapen avses vapen som konstruerats för att förinta stora människomassor, såsom exempelvis kemiska vapen, biologiska vapen och kärnvapen. Med hjälp av metoder för underrättelseinhämtning kan man i detta syfte skaffa information om till exempel förberedelser för eller planer på att tillverka eller förmedla massförstörelsevapen.

Enligt den föreslagna 4 punkten får metoder för underrättelseinhämtning användas för att inhämta information om planering, tillverkning, spridning och användning av sådana produkter med dubbel användning som avses i 2 § i lagen om kontroll av export av produkter med dubbel användning (562/1996).

Enligt 2 § i lagen om kontroll av export av produkter med dubbel användning avses med produkter med dubbel användning produkter, teknologi, tjänster och andra nyttigheter som vid sidan av sin normala civila användning eller tillämpning kan användas i syfte att utveckla eller tillverka massförstörelsevapen eller robotsystem för framförande av sådana till ett mål eller i syfte att främja den allmänna militära potentialen. Det viktigaste målet för exportkontrollen av sådana produkter är en politik som siktar på icke-spridning av massförstörelsevapen.

Planering, tillverkning, spridning och användning av produkter med dubbel användning kan ta sig uttryck exempelvis i att sådana produkter skaffas, transiteras eller distribueras i strid med den gällande lagstiftningen om exportkontroll, EU:s restriktioner eller FN-sanktioner. Information kan inhämtas till exempel om en utländsk aktörs intentioner, planer eller förberedelser att genom svikligt eller vilseledande förfarande skaffa produkter med dubbel användning av ett finskt företag i strid med EU-sanktioner eller FN-sanktioner.

Enligt 5 punkten får metoderna användas för att inhämta information om verksamhet som hotar den demokratiska samhällsordningen.

Enligt 2 § i grundlagen tillkommer statsmakten i Finland folket, som företräds av riksdagen. Till demokratin hör att den enskilde har rätt att ta del i och påverka samhällets och livsmiljöns utveckling. Med verksamhet som hotar den demokratiska samhällsordningen avses sådana strävanden att störta eller förändra demokratin där någon använder våldsmetoder, hot om våld, utpressning eller något annat förfaringssätt i strid med konstitutionen. Enligt Finlands grundlag innefattar grunderna för statsordningen utöver demokratin statsskicket, rättsstatsprincipen, fördelningen av statliga uppgifter och parlamentarismen. En central del av statens rättsordning utgörs av rättsnormerna, som styr samhällslivet (RP 188/2002 rd, s. 61).

Verksamhet som hotar den demokratiska samhällsordningen kan ta sig uttryck exempelvis i planer på att använda vapenmakt för att genomföra en statskupp eller revolution inom landet eller i planer på att ansluta Finland till en främmande makt. Som verksamhet som hotar den demokratiska samhällsordningen kan också anses exempelvis strävanden att genom våld förhindra riksdagen från att utöva sin lagstiftningsmakt eller tvinga de personer som utövar regeringsmakten att göra eller låta bli att göra något inom sina statliga uppdrag. Information kan inhämtas exempelvis om vilka planer eller förberedelser aktörer med sådana intentioner har och om vilka personer i Finland eller utomlands som deltar i sådan verksamhet. Det ska också anses som verksamhet som hotar den demokratiska samhällsordningen om någon agerar för att hindra eller störa dem som vill rösta i riksdagsval eller i valet av republikens president.

Enligt 6 punkten får metoderna användas för att inhämta information om verksamhet som hotar ett stort antal människors liv eller hälsa eller samhällets vitala funktioner.

Med verksamhet som hotar ett stort antal människors liv eller hälsa avses sådan verksamhet där det potentiella antalet offer innebär att verksamheten kan anses rikta sig mer allmänt mot samhället eller den kollektiva känslan av säkerhet. I motsats till i fallet terrorism definieras verksamheten här neutralt i fråga om avsikt på så sätt att den som står bakom hotet inte förutsätts ha ett visst ändamål. Hotet kan uppstå till exempel om någon anlägger en brand, spränger eller sprider farliga kemikalier eller genom annan liknande allmänfarlig verksamhet. Information ska kunna inhämtas om exempelvis planer eller andra förberedelser i samband med vilka någon skaffar sprängämnen eller på ett avvikande sätt skaffar kemikalier eller ämnen som kan användas för tillverkning av explosiva varor. Eftersom det krävs att den hotande verksamheten ska rikta sig mot ett stort antal människor ska civil underrättelseinhämtning med stöd av denna punkt inte kunna avse verksamhet som enbart hotar en enskild människa eller ett litet antal människor. Verksamhet som hotar liv eller hälsa för en enskild människas eller ett antal människor som utgör ett stort antal kan emellertid i enskilda fall utgöra exempelvis terrorism enligt 1 punkten eller verksamhet som hotar stats- eller samhällsordningen enligt 3 punkten. Det avgörande i detta fall är bland annat den hotande verksamhetens bakomliggande motiv och den eller de personernas ställning som hotet riktar sig mot inom den statliga beslutsprocessen..

De vitala samhällsfunktioner som avses i bestämmelsen är nödvändiga övergripande verksamheter som måste fungera i alla lägen. Till dessa hör bland annat statsledning, internationell verksamhet, rikets militära försvar, upprätthållande av inre säkerhet och fungerande ekonomi och infrastruktur. Med verksamhet som hotar dess vitala funktioner avses till exempel verksamhet som syftar till att kännbart försvaga eller avbryta funktionerna. Men hotet kan också utöver aktiv verksamhet bestå av sådana försummelser eller bieffekter av faktisk verksamhet som kan utsätta Finland för en miljökatastrof genom att hota luftens eller vattnets renhet eller orsaka höjd strålningsnivå. Information kan också inhämtas exempelvis om verksamhet där någon försöker avbryta eller förstöra sådana vitala samhällsfunktioner såsom elproduktion, vägtrafik och informationssystem, transportlogistik, samhällsteknik, livsmedelsförsörjning eller finans- och betalsystem. Exempelvis ska information då kunna inhämtas om förändringar i ägarförhållanden som äventyrar Finlands försörjningsberedskap eller om verksamhet där en främmande stat i it-systemen kartlägger den datatekniska strukturen på det europeiska nätet för energidistribution och tekniska sårbarheter i syfte att eventuellt utnyttja informationen för att slå ut elsystemet.

Enligt 7 punkten får metoderna användas för att inhämta information om en främmande stats verksamhet eller förberedelse av verksamhet som kan orsaka skada för Finlands internationella relationer eller ekonomiska intressen eller andra viktiga intressen,

Med sådan verksamhet av en främmande stat som orsakar skada avses exempelvis verksamhet som på ett fientligt sinnat sätt försöker påverka beslutsfattandet i Finland. Den metodarsenal som en främmande stat har för sådan påverkan kan vara bred och den kan beroende på det världspolitiska läget variera mellan allt från politiska och ekonomiska medel samt metoder för informationspåverkan ända till taktisk försummelse av myndighetsverksamhet eller exceptionell aktivitet som saknar faktisk grund i omvärlden.

Den främmande staten kan försöka genomföra gärningen på så sätt att den stat som är föremål för gärningen inte kan vara säker på om det är frågan om en målinriktad operation som styrs av den främmande staten eller inte. Sådan verksamhet kan exempelvis bestå i försök att påverka den allmänna opinionen i Finland eller utomlands genom systematisk spridning i offentligheten av falsk information om politiken i Finland. Information ska i så fall kunna inhämtas

om vilken eller vilka aktörer som står bakom den informationspåverkan som riktas mot Finland och om vad som är syftet med sådan verksamhet.

Enligt 8 punkten får metoderna användas för att inhämta information om kriser som hotar internationell fred och säkerhet.

Med sådana kriser avses till exempel en situation som eskalerat till en väpnad konflikt i en främmande stat eller handlingar som förebådar hot om att freden kan brytas. Hot mot internationell fred och säkerhet kan uppkomma dels genom väpnade konflikter, dels också av många olika slag av bidragande faktorer såsom befolkningsutvecklingen, migrationsströmmar mellan stater, matbrist eller knappa naturresurser. En kris som hotar internationell fred och säkerhet kan också uppkomma av auktoritära eller halvauktoritära regeringars och bräckliga demokratiers åtgärder där de begränsar de demokratiska institutionernas verksamhet och kringskär de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. För att hota internationell fred och säkerhet ska en kris a priori uträckas längre än bara inom en stat och den ska ha åtminstone regionala återverkningar på de kringliggande staterna. Information ska kunna inhämtas exempelvis om hur krisen eller det politiska läget i berörda främmande stater utvecklas eller om vilka säkerhetspolitiska konsekvenser krisen eventuellt kan leda till för Finlands del.

Enligt 9 punkten får metoderna användas för att inhämta information om verksamhet som hotar säkerheten vid internationella krishanteringsinsatser.

Enligt 1 § i lagen om civilpersonals deltagande i krishantering (1287/2004) deltar Finland i internationell krishantering bland annat för att förebygga och begränsa konflikter, avhjälpa de skador de åstadkommit och återställa ett fungerande samhälle samt för att lindra skadeverkningarna av storolyckor och naturkatastrofer. Bestämmelser om militär krishantering finns i lagen om militär krishantering (211/2006).

Information kan inhämtas om handlingar som hotar krishanteringsinsatser eller de deltagande personerna. Informationsinhämtningen kan då gälla exempelvis förhållandena på insatsområdena och faktorer som påverkar den utsända personalens säkerhet. De kan gälla huruvida den från Finland utsända personalen hotas av en våldsattack eller var, när och av vem eventuella våldsdåd är planerade att genomföras.

Enligt 10 punkten får metoderna användas för att inhämta information om verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och deltar i annan internationell verksamhet.

Stater, EU och internationella organisationer har skapat olika samordnings- och samarbetsmekanismer för att bekämpa och hantera hot mot den inre säkerheten. De bygger på bilaterala och multilaterala avtal och samarbetsmekanismer. Avsikten är att stater kan ge varandra samt EU och internationella organisationer stöd och bistånd till exempel vid terroristbrott, naturolyckor, katastrofer och andra nödlägen eller vid hot om sådana. I Lissabonfördraget stärktes EU-staternas solidariska ansvar genom att det till fördraget om Europeiska unionens funktionssätt fogas en s.k. solidaritetsklausul (FEUF artikel 222) för sådana situationer.

Inom inrikesministeriets förvaltningsområde finns en rad instrument på internationell nivå och EU-nivå som polis-, räddnings- och gränssäkerhetsmyndigheterna kan använda för bekämpning och hantering av hot och risker som gäller den inre säkerheten och genom vilka man kan lämna och ta emot stöd och bistånd. Exempel på samarbete som bygger på lagstiftningen på EU-nivå är unionens civilskyddsmekanism, det samarbete som koordineras av Europeiska gräns- och kustbevakningsbyrån (Frontex) och det s.k. Prümsamarbetet och Atlassamarbetet,

genom vilka man strävar efter att effektivisera samarbetet mellan rättsvårdande myndigheter och polismyndigheter i syfte att bekämpa terrorism och gränsöverskridande brottslighet.

Med verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och deltar i annan internationell verksamhet enligt 10 punkten avses sådan verksamhet eller förberedelse av verksamhet från en främmande stats eller enskild aktörs sida vars syfte är att skada exempelvis polisens sambandsmän eller andra personer som staten sänt utomlands. Information ska kunna inhämtas om huruvida det finns säkerhetshot mot dem som deltar i internationella stöd- och biståndsinsatser.

Enligt 11 punkten får metoderna användas för att inhämta information om internationell organiserad brottslighet som hotar samhällsordningen.

Här avsedd verksamhet kan exempelvis bestå i att den internationella organiserade brottsligheten infiltrerar statsförvaltningen och tar över centrala tjänster för att på det sättet påverka viktiga samhällsbeslut eller till exempel skaffa sig ekonomiskt eller politiskt inflytande genom köp av samhällsviktig infrastruktur eller samhällsvitala funktioner såsom elproduktion, avfallshantering eller transport- och speditionsföretag.

4 §. *Förutsättningar för användning av metoderna för underrättelseinhämtning.* I 1 mom. anges som ett för alla metoder allmänt villkor för användning, dvs. att ”man med den med fog kan antas få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten”. Det är fråga om ett krav på resultat som ska motiveras, och då utgår man från att användningen av metoden för underrättelseinhämtning ger den nytta den motiverats med. Nyttan med att metoden används måste kunna motiveras i varje enskilt fall, vilket framgår av uttrycket ”med fog”. Motiveringen kan hänga samman exempelvis med varför en viss person eller grupp av personer eller en viss lokal eller något annat ställe måste kunna observeras och varför man på det sättet kan förvänta sig att få information som gagnar den nationella säkerheten. Det kan hänga samman med bland annat personens eller gruppens beteende eller med annan relevant information. Med verksamhet som är föremål för civil underrättelseinhämtning avses verksamhet enligt 3 § (Föremål för civil underrättelseinhämtning). Den grundläggande förutsättningen är också kopplad till att det finns grundad anledning att börja skydda sig mot den verksamhet som avses i 3 §.

Kravet på att verksamheten allvarligt ska hota den nationella säkerheten beror på det 4 mom. som kommer att föreslås till 10 § i grundlagen. Den grundlagsbestämmelsen innebär att kravet på allvarligt hot höjer tröskeln för tillämpning av metoder som ingriper i skyddet för förtroliga meddelanden när hotets kvalitet ska anges. Det innebär att det inte räcker med verksamhet som utgör någon form av hot mot den nationella säkerheten för att uppfylla det krav bestämmelsen ställer. Hotets allvarlighetsgrad är också kopplad till de ovan i 3 § behandlade innehållsmässiga definitionerna om hurdan verksamheten ska vara för att utgöra ett allvarligt hot mot den nationella säkerheten.

De verksamheter som allvarligt kan hota den nationella säkerheten ingår uttömmande i de föremål för civil underrättelseinhämtning som avses i 3 §. Det räcker emellertid inte med ett hot på abstrakt nivå för att metoder för underrättelseinhämtning ska få användas, utan det ska i det enskilda fallet gå att visa att den verksamhet som den civila underrättelseinhämtningen riktas mot utgör eller kan antas utgöra ett allvarligt hot mot den nationella säkerheten. Detta framgår av relativsatsen ”som allvarligt hotar den nationella säkerheten”. Ordet ”hotar” betyder att bestämmelsen inte kräver att den nationella säkerheten ska vara direkt äventyrad. Med andra ord kan inhämtande av information enligt den bestämmelsen också avse verksamhet som är föremål för civil underrättelseinhämtning och som, om den fortsätter, allvarligt kommer att hota den nationella säkerheten. Det krävs emellertid att hotet i någon grad ligger nära tidsmässigt

eller att det har åtminstone en indirekt koppling till Finlands nationella säkerhet. Som ett exempel kan nämnas att en kris som hotar internationell fred och säkerhet inte hotar den nationella säkerheten, om den saknar beröringspunkter med Finland eller inte ens kan antas sprida sig till Finland eller komma att beröra Finland. I fråga om terrorism kan man däremot i flera fall anta att attacker som skett i Finlands grannländer, Europa eller någon annanstans kan komma att spridas också till finskt territorium. Inhämtningen av information innefattar också kartläggning av externa hot mot Finland. Det vore således exempelvis fråga om att följa hur den säkerhetspolitiska miljön utvecklas så att man kan få en lägesbild av den nationella säkerheten.

Att uttrycket ”den nationella säkerheten” används betyder att den hotande verksamhet som avses i bestämmelsen inte primärt riktas mot någon som individ utan mer allmänt mot samhället och dess medlemmar som kollektiv. Men samtidigt kan våldsdåd som riktas mot enskilda individer vara i bestämmelsen avsedd verksamhet, om dåden till sin omfattning eller betydelse är relevanta med avseende på den nationella säkerheten och därmed kan komma att utgöra ett allvarligt hot mot den. Det är självskrivet att hot mot exempelvis statsledningen eller dem som ansvarar för samhällets grundläggande funktioner och dem som svarar för dessa personer säkerhet kan utgöra ett allvarligt hot mot den nationella säkerheten. Definitionen av nationell säkerhet behandlas närmare i den proposition där det föreslås att 10 § 3 mom. i grundlagen ska ändras. I den allmänna motiveringen behandlas de ställningstaganden om den nationella säkerheten som framgår av Europadomstolens avgörandepraxis. Av den framgår också begreppets föränderliga och i vissa fall oförutsägbara karaktär.

Uttrycket ”med fog kan antas” uttrycker motsvarande grad av sannolikhet som det numera i brottsbaserade fullmakter använda ”finns skäl att anta” eller ”finns skäl att misstänka” (alt. ”finns anledning att misstänka”), som används för att uttrycka grad av sannolikhet vid användning av hemliga tvångsmedel. Numera uttrycks den lägsta graden av sannolikhet med ”finns skäl att anta”, som exempelvis beskriver förutsättningarna för beslag i 7 kap. 1 § i tvångsmedelslagen. Bland parallelluttrycken till ”finns skäl att anta” kan nämnas ”finns anledning att misstänka” och ”är skäligen misstänkt” i tvångsmedelslagens 6 kap. 1 §, som gäller förutsättningar för kvarstad. Sådana uttryck används när det är fråga om mänskliga gärningar som antingen redan har skett (t.ex. ett brott) eller antas kunna ske i framtiden (t.ex. undvikande av förundersökning). Uttrycket ”finns skäl att misstänka” används också i 3 kap. 3 § 1 mom. i förundersökningslagen. Paragrafen anger när förundersökning ska göras. Enligt motiven i RP 14/1985 (s. 16) finns det skäl att misstänka ett brott när en omsorgsfull person på grund av sina iakttagelser kommer till en sådan slutsats.

Dessutom ska metoden för underrättelseinhämtning kunna inriktas så exakt som möjligt. Det kravet beror på polisrättsliga principer, särskilt principen om minsta olägenhet.

I 2 mom. anges särskilda förutsättningar för användning av de olika metoderna för underrättelseinhämtning. Enligt första meningen i momentet får teleavlyssning, inhämtande av information i stället för teleavlyssning, systematisk observation, teknisk avlyssning, optisk observation, teknisk spårning av personer, teknisk observation av utrustning, täckoperationer, bevisprovokation genom köp, styrd användning av informationskällor och platsspecifik underrättelseinhämtning användas endast om dessa metoder med fog kan antas vara av synnerlig vikt för att få information om sådan verksamhet som avses i 1 mom. Enligt andra meningen förutsätts för täckoperationer och bevisprovokation genom köp dessutom att användningen av metoden är nödvändig. Vidare sägs det i tredje meningen att en förutsättning för täckoperationer dessutom är att inhämtandet av information måste anses vara behövligt på grund av att verksamheten är planmässig, organiserad eller yrkesmässig eller på grund av att det kan antas att den fortsätter eller upprepas.

Uttrycken ”av synnerlig vikt” och ”nödvändig” i 4 § motsvarar uttrycken i fråga om förutsättningar för användning av hemliga metoder för inhämtande av information, som det föreskrivs om i 5 kap. 2 §. I propositionen om den gällande polislagen (RP 224/2010 rd, s. 40–45 och 94 och 95) finns en närmare genomgång av vad som avses med uttrycken ”av synnerlig vikt” (alt. ”synnerligen stor betydelse”) och ”nödvändig” i den del av motiveringen som gäller förutsättningarna för användning av metoder för inhämtande av information.

Av täckoperationer krävs utöver nödvändighet att den riktar sig mot organiserad verksamhet som allvarligt hotar den nationella säkerheten. Planmässighet är ofta kopplad till organiserad verksamhet. Att planmässighet nämns innebär också att metoden också fortsättningsvis kan riktas mot till exempel en och samma enskilda aktörs planmässiga verksamhet. Ett annat villkor för användning av täckoperationer avses vara att metoden behöver användas för att den verksamhet som allvarligt hotar den nationella säkerheten kan antas fortsätta eller upprepas. Med detta avses att verksamheten inte behöver vara planmässig, organiserad eller yrkesmässig, men antagligen kontinuerlig eller upprepad, och då kan det vara fråga om något sådant som en enskild icke-organiserad person.

Användningen av täckoperationer begränsas i 4 mom. av ett förbud mot att rikta metoder för underrättelseinhämtning mot ett utrymme som används för stadigvarande boende. Befogenheten att företa täckoperationer ger inte rätt till tillträde till sådana utrymmen. Samtidigt bör den som deltar i en täckoperation ha rätt att inträda i sådana utrymmen för att inte avslöjas och att då dra nytta av täckmanteln. En polisman som utför en täckoperation kan för det mesta svårligen i sådana situationer avböja att gå in i en bostadslägenhet utan att avslöjas. Att avslöjas kan innebära risk för den deltagande personens liv eller hälsa. Dessutom kan detta erbjuda möjlighet att testa om det är fråga om en person som deltar i en täckoperation eller inte. Samtidigt bör man i täckoperationer försöka undvika situationer där operationen inbegriper besök i utrymmen som används för stadigvarande boende. Det krävs då noggrann planering av täckoperationen.

Utöver för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning eller kopiering av försändelser ska även villkoren för kopiering vara striktare när kopieringen gäller meddelanden. Med meddelanden avses då uttryckligen förtroliga meddelanden som skyddas genom 10 § i grundlagen. Kopieringen riktar sig mot meddelandet åtminstone när kopieringen gäller ett brev som lämnats på ett bord eller ett e-postmeddelande som syns på datorskärmen. I sådana fall krävs det att villkoren i första meningen är uppfyllda för att meddelandet ska få fotograferas eller kopieras på annat sätt. Däremot blir de kvalificerade villkoren för kopiering inte tillämpliga om polisen känner till att den försändelse som är föremål för kopiering av försändelse inte innehåller ett sådant meddelande.

I 3 mom. föreslås bestämmelser om en lägre tröskel för användning av metoder när den riktar sig mot statliga aktörer eller med sådana jämställbara aktörer. I fråga om metoder för underrättelseinhämtning som inkräktar i skyddet för förtroliga meddelanden betyder detta att till exempel teleavlyssning kan gälla kommunikationen mellan två statliga aktörer, om denna kommunikation inte omfattas av skyddet för förtroliga meddelanden enligt grundlagen. En sådan situation kan råda exempelvis när kommunikationen sker i ett myndighetsnät. Om en offentliganställd tjänsteman använder ett myndighetsnät för sina privatsamtal tar han eller hon samtidigt den risken att den andra kommunikationsparten också kan bli föremål för underrättelseinhämtning. Utgångspunkten är att myndighetsnät används bara för kommunikation mellan myndigheter.

Med situationer där myndigheter agerar jämställs situationer där det till exempel i en stat inte finns aktörer som inte i sig kan identifieras som myndigheter, men som utför statliga uppdrag på samma sätt som en myndighet. Den aktören kan bedömas exempelvis utifrån huruvida Fin-

land eller en finländsk myndighet skulle kunna ingå ett avtal med aktören eller om aktören kan delta i en internationell organisations verksamhet.

Med en aktör som kan jämställas med en myndighet avses också den som agerar för en myndighet, dvs. en mellanhand som handlar helt och hållet för den statliga aktörens räkning. Det kan röra sig om privata aktörer såsom företag, om andra grupperingar eller till och med om enskilda personer. Det är då av väsentlig vikt att bedöma till exempel om den sådan aktör handlar under statens bestämmande inflytande eller i dess styrning eller om staten tar på sig ansvaret för en sådan aktörs handlande. Det går, för att ge ett exempel, inte att anse att ett företag är en statlig aktör om det på grundval av ett kommersiellt privaträttsligt avtal har skyldigheter gentemot en statlig aktör. Det som måste beaktas är hurdant statens bestämmande inflytande eller hurdan dess styrning är i fråga om företaget och hur konkret staten kan bestämma företagets verksamhet.

När det gäller andra grupperingar ska man dessutom beakta hur organiserad verksamheten är, hur stora resurser grupperingen har exempelvis för en väpnad attack och huruvida en sådan attack till sina effekter kan jämställas med en attack genomförd av en främmande stat samt huruvida grupperingen försöker agera som en stat.

Det säger sig självt att en statlig aktör redan i förväg har konstaterats vara en sådan och att aktörens statliga ställning är uppenbar. Detta innebär att skyddspolisen när den beslutar om användning av en metod för underrättelseinhämtning eller gör upp tillståndsyrkandet ska ha en förhandsuppgift om att det rör sig om en statlig aktör och att objektet medan metoden används agerar i egenskap av en sådan. Det kan hända att metoden i början gäller inhämtande av information om en icke-statlig aktör, men att användningen av metoden senare kan komma att gälla en statlig aktör utifrån de uppgifter som metoden ger, om det uppenbart visar sig att aktören har statlig status. I sista hand är det den som fattar beslutet som måste avgöra om det har presenterats tillräckligt med fakta som stöder uppfattningen att objektet kan anses vara en statlig aktör.

Enligt det föreslagna 4 mom. får metoder för underrättelseinhämtning inte riktas mot ett utrymme som används för stadigvarande boende. Grundlagsskyddet för hemfriden täcker i princip in alla typer av utrymmen som används för boende av permanent natur (t.ex. GrUU 43/2010 rd, s. 2, GrUU 40/2010 rd, s. 4, GrUU 18/2010 rd, s. 7, GrUU 6/2010 rd, s. 4, och GrUU 8/2006 rd). Den sfär som omfattas av hemfriden definieras inte på samma sätt i grundlagen som till exempel i strafflagen. Det innebär att en metod för underrättelseinhämtning inte får riktas mot en sådan hemfridsskyddad bostad eller övriga utrymmen som är avsedda för boende som avses i 24 kap. 11 § i strafflagen, såvida det inte går att visa att platsen faktiskt används för annat än boende av permanent natur (GrUU 36/1998 rd och HD 2009:54). De enda undantagen är täckoperationer och bevisprovokation genom köp, där en tjänsteman vid skyddspolisen som deltar i täckoperationen eller bevisprovokationen måste ha rätt att inträda i sådana utrymmen för att inte avslöjas och att då dra nytta av täckmanteln. Därför står det momentet att en täckoperation eller bevisprovokation genom köp dock får företas i en bostad om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden. Det är med tanke på rättssäkerheten motiverat att utsträcka denna regel också till bevisprovokation genom köp, eftersom sådana köp också kan genomföras i en bostad.

Enligt det föreslagna 5 mom. ska användning av en metod för underrättelseinhämtning avslutas före utgången av den tid som anges i beslutet, om syftet med användningen har nåtts eller om det inte längre finns förutsättningar för att använda metoden. På detta sätt understryks det att metoderna inte under några omständigheter får användas längre än vad som behövs även om tillståndet fortfarande gäller. Det är klart att användningen av en metod för underrättelseinhämtning måste upphöra senast när tillståndet upphör att gälla.

Metoderna definieras i 5 kap., med undantag för platsspecifik underrättelseinhämtning, kopiering, kvarhållande av försändelser för kopiering och underrättelseinhämtning som avser datatrafik, och bestämmelserna om förutsättningar och föremål för användning av metoderna och om det berörda beslutsfattandet avses finnas i 5 a kap. och i lagen om civil underrättelseinhämtning avseende datatrafik.

De polisrättsliga principerna är extra accentuerade när metoder för underrättelseinhämtning används. Respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna, proportionalitet, strävan efter minsta möjliga olägenhet och ändamålsbundenhet är alla viktiga principer när metoderna används. Iakttagande av dessa principer i samband med civil underrättelseinhämtning bidrar till att tolkningen av förutsättningarna för användning av metoderna för underrättelseinhämtning hålls inom givna ramar.

Grundlagsutskottet har i sina utlåtanden (GrUU 32/2013, s. 4, och GrUU 33/2013, s. 4) understrukit att de allmänna principerna i polislagen och tvångsmedelslagen liksom även de allmänna och särskilda förutsättningarna för användning av hemliga metoder för informationsinhämtning och av hemliga tvångsmedel ska vägas in såväl när tillstånd söks som när det beviljas av domstol (se även HD 2007:7 och HD 2009:54). Det går inte att differentiera förutsättningarna för användning av metoderna utifrån huruvida brottet uppfyller kriterierna för att en viss påföljd ska kunna utdömas, vilket ger beslutsfattaren accentuerad rätt till information för att kunna bedöma tillståndsvillkoren. Beslutsfattaren måste i dessa fall ha tillgång till tillräckligt med information för att ha möjlighet att noggrant bedöma behovet av ett tillstånd och tillståndets räckvidd.

5 §. *Fortsatt inhämtande av information för avslöjande och förhindrande av vissa brott* Paragrafen avses innehålla bestämmelser om användning av metoder för underrättelseinhämtning i sådana fall där det finns ett behov av fortsatt inhämtande av information för avslöjande eller förhindrande av vissa brott. Skyddspolisen ska få fortsätta att inhämta information för att förhindra eller avslöja ett brott under giltighetstiden för ett tillstånd eller beslut enligt 5 a kap., om det medan en metod för underrättelseinhämtning används i samband med civil underrättelseinhämtning framkommer att en person med fog kan antas göra sig skyldig till ett brott som nämns i 5 kap. 3 § eller till högförräderi, grovt högförräderi eller olaglig militär verksamhet eller det kan antas att ett sådant brott har begåtts och det genom användning av metoden för underrättelseinhämtning inte längre kan antas att man får information om verksamhet som allvarligt hotar den nationella säkerheten och som låg till grund för tillståndet eller beslutet.

Paragrafen gäller således fortsatt användning av en relevant metod med anledning av nationell säkerhet i syfte att förhindra eller avslöja landsförräderibrott, högförräderibrott, och terroristbrott, för vilket skyddspolisens ansvarar, till skillnad från de fall som avses i 5 kap. 4 §. I de fallen är det fråga om fortsatt hemligt inhämtande av information för utredning av ett brott vilket om helst som inhämtandet gäller. Eftersom hänvisningen till 5 kap. 3 § bara täcker in landsförräderibrott och terroristbrott nämns vissa högförräderibrott särskilt i 5 §. Genom paragrafen blir det möjligt att använda sig av metoder för underrättelseinhämtning under den tid ett tillstånd eller beslut om detta är i kraft, när en grund enligt 5 a kap. för användningen inte längre finns men det finns ett behov av fortsatt informationsinhämtning för att förhindra eller avslöja ett brott. Utan den föreslagna paragrafen skulle skyddspolisen bli tvungen att upphöra med användningen exempelvis när det intresse för underrättelseinhämtning som den nationella säkerheten gav upphov till blir smalare och bara gäller ett intresse att inhämta information för att förhindra eller avslöja ett brott.

Det ska med stöd av paragrafen vara tillåtet att under den tid tillståndet gäller fortsätta sådan användningen av en metod som inletts med stöd av 5 a kap., men inte längre än en månad. Detta innebär att metoden får användas i ytterligare två dagar om det ursprungliga tillståndet

gäller i två dagar till och att metoden får användas i en månad om det ursprungliga tillståndet gäller i mer än månad till. Efter det måste tillstånd eller beslut sökas enligt 5 kap. eller användningen av metoden för underrättelseinhämtning upphöra.

Det ska inte vara tillåtet att fortsätta med platsspecifik underrättelseinhämtning, kopiering eller kvarhållande av försändelser för kopiering med stöd av paragrafen för att förhindra eller avslöja brott, eftersom det inte finns bestämmelser om motsvarande metoder för inhämtande av information i 5 kap. i polislagen.

Däremot ska skyddspolisen få fortsätta använda metoden enligt detta kapitel också den tid som förlängt tillstånd eller beslut gäller i de situationer där den verksamhet som allvarligt hotar den nationella säkerheten inte utmynnar i ett separat enstaka landsförräderibrott, högförräderibrott eller terroristbrott. Det är med andra ord fråga om att sådan användning av metoder för underrättelseinhämtning som sker med tanke på den nationella säkerheten får fortsätta inom ramen för meddelade tillstånd eller beslut så länge sådan informationsinhämtning fortfarande kan antas ge upplysningar om verksamhet som allvarligt hotar den nationella säkerheten.

6 §. *Beslut om teleavlyssning och motsvarande inhämtande av information vid civil underrättelseinhämtning.* Enligt 1 mom. ska beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning vid civil underrättelseinhämtning fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Bestämmelser om domstolsbehandlingen av yrkandet finns i 35 §. Beslutet ska fattas på samma nivå som i fråga om 5 kap.

Enligt första meningen i 2 mom. kan tillstånd till teleavlyssning eller inhämtande av information i stället för teleavlyssning ges för högst sex månader åt gången. Tillståndet ska kunna gälla lägre än i fråga om teleavlyssning enligt 5 kap., där tillstånd kan ges för högst en månad åt gången. Den längre tiden är motiverad med tanke på den civila underrättelseinhämtningens karaktär och grunden för användning av metoderna för underrättelseinhämtning. Underrättelseverksamhet är av en märkbart annan karaktär än brottsbekämpningens behov. Om det efter sex månader krävs fortsatt användning av metoden har också domstolen i samband med den nya behandlingen en äkta möjlighet att kontrollera om förutsättningarna för tillståndet fortfarande uppfylls utan att rättssäkerheten äventyras.

Metoderna för underrättelseinhämtning ska inte få användas för att förhindra, avslöja eller utreda enskilda brott och de upplysningar som inhämtas med metoderna ska inte få användas inom brottsbekämpning annat än uteslutande under de förutsättningar som anges i 44 §. Underrättelseinhämtning pågår ofta längre än brottsbekämpning och insatserna är ofta noga planerade i förväg. En insats kan exempelvis syfta till att samla upplysningar om målstatsverksamhet som skadar Finlands intressen och relaterade omständigheter. Omfattande operationer för underrättelseinhämtning kan vara väldigt långvariga. Syftet är då inte att förhindra eller utreda ett enstaka brott utan att i ett tidigt skede samla in information för att få en samlad bild av läget. Bestämmelsen medger således föregripande och mer långvarig inhämtning av information med ett enda tillståndsbeslut.

Den föreslagna längden på tillståndet, sex månader, betyder emellertid inte automatiskt att tillstånd alltid kan sökas för sex månader eller att den ska beviljas för sex månader. Uttrycket ”för högst sex månader åt gången” ska i bestämmelsen tolkas som ett krav på prövning enligt proportionalitetsprincipen och principen om minsta olägenhet. Därför ska den som ansöker om tillstånd eller beviljar tillstånd i varje enskilt fall tänka igenom hur längre metoden behöver användas.

Enligt andra meningen i 2 mom. ska tillstånd kunna beviljas för högst tre månader åt gången när åtgärden gäller en person. Vid teleavlyssning (och teleövervakning) ska föremålet för åtgärden med avvikelse från 5 kap. utöver en teleadress eller teleterminalutrustning också kunna vara en person. I sådana fall är det motiverat att tillämpa en kortare tillståndstid. Om det behövs förlängning efter tre månader av teleavlyssning ger en ny behandling också domstolen en äkta möjlighet att kontrollera hur teleavlyssningen bör riktas. Redan det faktum att till exempel underrättelseombudsmannen inte ingripit i användningen av teleavlyssning skulle vara ett uttryck för att användningen är godtagbar och följer lag.

I 3 mom. föreslås bestämmelser om vilka uppgifter som ska ingå i yrkandet och beslutet. Enligt 1 punkten ska yrkandet och beslutet nämna den verksamhet som avses i 3 § och som allvarligt hotar nationell säkerhet. Åtminstone ett av de föremål som avses i 3 § ska således nämnas som grund för användning av metoden för underrättelseinhämtning.

I 2 punkten anges det att yrkandet och beslutet ska ange det objekt som metoden riktas mot, dvs. i fråga om teleavlyssning en person, teleadress eller teleterminalutrustning. Till skillnad från teleavlyssning enligt 5 kap. 5 § i polislagen och 10 kap. 3 § i tvångsmedelslagen kan också en person vara föremål för teleavlyssning vid civil underrättelseinhämtning. När tillståndet till teleavlyssning avser en person gäller det de teleadresser och den teleterminalutrustning som den berörda personen har i sin besittning eller medan tillståndet gäller får i sin besittning eller som personen i övrigt kan antas använda. Teleavlyssningstillståndet är således inte knutet till en viss teleadress eller till viss teleterminalutrustning. Den som ansöker om tillstånd ska emellertid kunna peka på grunderna för att personen i fråga antas förfoga över information som är av betydelse för den nationella säkerheten. När den person som avses i domstolens tillstånd och som är föremål för åtgärden börjar använda eller antas ha börjat använda en ny teleadress eller ny teleterminalutrustning eller när det framkommer att personen har en teleadress eller teleterminalutrustning som inte anges särskilt i tillståndsansökan till domstolen ska underrättelsemyndigheten kunna rikta in åtgärden på dessa. Också i fråga om sådana adresser och sådan utrustning ska underrättelseombudsmannen underrättas.

Den föreslagna 3 punkten är viktig med tanke på beslutsfattandet. Enligt den ska yrkandet och beslutet ange de fakta som förutsättningarna för och inriktningen av teleavlyssningen eller inhämtningen av information i stället för teleavlyssning grundar sig på. Den punkten ålägger skyddspolisen att presentera och motivera fakta på ett sätt som ger domstolen en faktisk möjlighet till en omsorgsfull tillståndsprövning. Domstolen kan då dra sina egna slutsatser om huruvida förutsättningarna uppfylls för användning av metoden för underrättelseinhämtning. De förutsättningar som avses är för det första de allmänna förutsättningar för användning av metoder för underrättelseinhämtning som anges i 5 a kap. 4 §. Dessutom ska yrkandet och beslutet ange tillräckliga fakta om vilken verksamhet enligt 3 § som allvarligt hotar den nationella säkerheten det är fråga om och varför tillståndet ska gälla den ansökta tiden. De polisrättsliga principerna ska accentueras särskilt när tillstånd söks och beslut motiveras.

Enligt 4 punkten ska yrkandet och beslutet ange giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning eller till inhämtande av information i stället för teleavlyssning. Angivande av klockslag krävs inte när information inhämtas i stället för teleavlyssning.

Enligt 5 punkten ska yrkandet och beslutet ange den polisman som hör till befälet vid skyddspolisen och som leder och övervakar utförandet av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.

Enligt 6 punkten ska yrkandet och beslutet ange eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning. Domstolen kan i sitt

beslut införa begränsningar och villkor för användningen av teleavlyssning. Om sådana begränsningar eller villkor är kända redan när yrkandet utarbetas ska de anges i yrkandet.

7 §. *Beslut om teleövervakning vid civil underrättelseinhämtning.* Enligt 1 mom. ska beslut om teleövervakning vid civil underrättelseinhämtning fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ett ärende som gäller teleövervakning inte tål uppskov, får chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om teleövervakning till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.

Den beslutanderätt som avses i momentet motsvarar delvis det som sägs i 5 kap. 10 § 1 och 2 mom. i den gällande lagen. Om chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning i ett brådskande läge har beslutat om teleövervakning och om domstolen anser att det inte fanns förutsättningar för ett sådant beslut måste användningen av den metoden avslutas och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas (46 §). Information som fåtts på detta sätt får dock användas på samma villkor som information får användas enligt 44 § 1 mom.

Kravet på förtrogenhet för den polisman som hör till befälet vid skyddspolisen avviker dock något från utbildningskravet i 5 kap. Grunderna för användning av metoderna för underrättelseinhämtning och de ibland otydliga gränserna mellan olika metoder innebär att det av en polisman som hör till befälet vid skyddspolisen bör krävas tillräcklig färdighetsnivå för användning av metoderna. Chefen för skyddspolisen hör självfallet till befälet och det gör även biträdande chefer för skyddspolisen och avdelningschefer, polisjurister, överinspektörer och inspektörer vid skyddspolisen. För att dessa tjänstemän ska ha kunna få självständig beslutanderätt i saken ska de också vara förordnade för uppdraget och förtrogna med användningen av metoder för underrättelseinhämtning. Kravet på förtrogenhet kan uppfyllas antingen genom utbildning i hemligt inhämtande av information eller genom tillräcklig erfarenhet av tillämpningen av sådant inhämtande. Dessutom bör polismannen vara insatt i den lagstiftning som gäller underrättelsebefogenheter. Innan den gällande polislagen och tvångsmedelslagen trädde i kraft och även efter det att lagarna hade trätt i kraft har polisförvaltningen ordnat utbildning för anhållningsberättigade tjänstemän med specialutbildning i hemlig informationsinhämtning (s.k. Stekpov-utbildning efter den finska förkortningen på utbildningen). Syftet med utbildningen har varit att ge anhållningsberättigade polismän bättre yrkesmässiga förutsättningar att använda hemliga metoder för inhämtande av information och hemliga tvångsmedel. Den typen av utbildning skulle också göra deltagarna förtrogna med användningen av metoderna för underrättelseinhämtning.

Ett brådskande beslut av chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning ska föras till domstol även om teleövervakningen avslutas inom 24 timmar efter det att metoden började användas. Annars skulle det vara möjligt att kringgå kraven på beslutsprocessen genom att inhämta information bara under kort tid. Det främjar lagenligt handlande när ärendet förs till domstol också i sådana fall. Detta ska även gälla andra situationer där chefen för skyddspolisen eller den förordnade och i metoderna insatta polismannen som hör till befälet temporärt kan besluta om användning av metoder för underrättelseinhämtning.

I 2 mom. finns bestämmelser om teleövervakning baserad på samtycke. Polisen ska få rikta teleövervakningen mot en teleadress eller teleterminalutrustning som innehas av en viss person,

om den med fog kan antas ha mycket stor betydelse när det gäller att få information om den verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten.

Med innehav av en teleadress eller teleterminalutrustning avses i så fall faktisk besittning. Det innebär till exempel att arbetsgivaren inte får ge sitt samtycke till teleövervakning av en mobiltelefon som en anställd använder. Inte heller sporadisk användning av någon annans mobiltelefon ger rätt till att ge samtycke i fråga om telefonägarens kommunikation. Samtycket ska ges skriftligen. I brådskande fall kan samtycket emellertid ges muntligt, men då ska det bekräftas skriftligt så snabbt som möjligt.

Enligt den rådande uppfattningen i doktrinen kan var och en på ett giltigt sätt ge sitt samtycke till teleövervakning av en teleadress eller teleterminalutrustning i sin besittning, men samtycket ska ges före åtgärden och vara genuint frivilligt och den som ger samtycket ska ha insett dess betydelse. Skyddspolisen får inte utöva påtryckning eller sätt ställa ledande frågor för att få samtycket. Polisen kan nämna möjligheten att använda samtyckesbaserad teleövervakning, men den berörda personen ska alltid själv få dra sina slutsatser om användningen av en viss metod för inhämtande av information (RP 224/2010 rd, s. 103–104).

Enligt 3 mom. ska chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om den teleövervakning som avses i 2 mom.

Enligt 4 mom. får tillstånd beviljas och beslut fattas för högst sex månader åt gången, och tillståndet eller beslutet får gälla även en viss tid före tillståndet beviljades eller beslutet fattades, vilken kan vara längre än sex månader. I fråga om tillståndets giltighetstid är det som framförs i motiveringen till 6 § 2 mom. huvudsakligen relevant.

I 7 § 5 mom. avses det finnas bestämmelser om vad som ska nämnas i yrkanden och beslut om teleövervakning. I detta avseende är det som framförs i motiveringen till 6 § 3 mom. relevant.

8 §. *Beslut om inhämtande av basstationsuppgifter vid civil underrättelseinhämtning.* Enligt 1 mom. ska beslut om inhämtande av basstationsuppgifter fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en polisman som hör till befälet vid skyddspolisen besluta om inhämtande av basstationsuppgifter till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.

Att inhämta basstationsuppgifter innebär ett mindre intrång i skyddet för förtroliga meddelanden än teleövervakning. Om en polisman som hör till befälet vid skyddspolisen i ett brådskande läge har beslutat om sådant inhämtande och om domstolen anser att det inte fanns förutsättningar för ett sådant beslut måste användningen av den metoden avslutas och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas (46 §). Information som fåtts på detta sätt får dock användas på samma villkor som information får användas enligt 44 § 1, 2 och 3 mom.

Enligt det föreslagna 2 mom. beviljas tillstånd för en viss tidsperiod. I sak motsvarar momenten 5 kap. 12 § 2 mom.

I 3 mom. föreslås bestämmelser om vilka uppgifter som ska nämnas i yrkandet och beslutet. I detta avseende är det som framförs i motiveringen till 6 § 3 mom. huvudsakligen relevant. Inhämtande av basstationsuppgifter är inte särskilt knutet till en viss person utan till en viktig tidpunkt och plats med avseende på den nationella säkerheten, och då räcker det med angi-

vande av de fakta som gäller i 3 § avsedd verksamhet. I yrkandet och beslutet ska det också motiveras varför basstationsuppgifterna ska inhämtas en viss tid och vad man försöker ta reda på genom att inhämta basstationsuppgifter. I ljuset av proportionalitetsprincipen kan perioden för inhämtandet inte vara längre än sex månader annat än i ytterst exceptionella fall.

9 §. *Beslut om systematisk observation vid civil underrättelseinhämtning.* Enligt 1 mom. ska beslut om systematisk observation vid civil underrättelseinhämtning fattas av en polisman som hör till befälet vid skyddspolisen.

I 2 mom. sägs det att beslut om systematisk observation får fattas för högst sex månader åt gången. I detta avseende är det som framförs i motiveringen till 6 § 2 mom. relevant.

I 3 mom. föreslås bestämmelser om vilka uppgifter som ska nämnas i yrkandet och beslutet. I detta avseende är det som framförs i motiveringen till 6 § 3 mom. huvudsakligen relevant. Den systematiska observationen ska enligt 2 punkten kunna gälla en grupp av personer. Det kan inom civil underrättelseinhämtning uppstå ett behov att följa en viss persongrupps agerande. Vid systematisk observation grundar sig informationsinhämtningen på en mer passiv typ av kontakter.

När denna metod för underrättelseinhämtning används är det inte fråga om åtgärder som siktar på att förhindra, avslöja eller utreda brott. Det innebär att identifiering av en viss person i samband med civil underrättelseinhämtning inte ger upphov till ett motsvarande behov att bedöma de särskilda förutsättningarna för utövande av befogenheten, dvs. om det exempelvis finns anledning att misstänka den berörda personen för ett brott där en viss påföljd kan utdömas eller om denne kan antas göra sig skyldig till ett sådant. Syftet med denna metod för underrättelseinhämtning kan till exempel vara att inhämta information om hur en viss grupp av personer är organiserad, om vilka som hör till gruppen, om gruppens aktivitet på vissa områden och om de olika formerna för gruppens verksamhet.

För att det ska vara fråga om en grupp av personer ska den bestå av minst tre personer. Dessa personer ska under en viss tid utgöra en strukturerad grupp som handlar i samförstånd eller åtminstone har ett gemensamt mål, t.ex. att sätta skräck i befolkningen eller att inhämta information om Finlands utrikes- och säkerhetspolitiska beslutsfattande. Den verksamhet som en grupp av personer bedriver är en form av organisationskultur som kan ta sig uttryck i synliga strukturer, som t.ex. orderkedjor mellan gruppens medlemmar, vissa värderingar och normer samt grundläggande antaganden såsom uppfattningar och övertygelser. För att en enskild person ska anses höra till en grupp av personer ska personen agera i enlighet med gruppens mål eller åtminstone främja förverkligandet av målen på ett betydande sätt. En grupp av personer kan exempelvis bestå av underrättelseofficerarna i en viss utländsk underrättelsetjänst.

Enligt principen om minsta olägenhet ska utövandet av befogenheten i första hand riktas mot en viss person. Inom underrättelseverksamhet kan det ändå finnas ett behov att utreda vilka som hör till en viss grupp eller hurdan verksamhet en viss grupp bedriver inom ett visst område. Det kan då röra sig om personer i en terroristgrupp eller inom en främmande underrättelsetjänsts organisation. När information inhämtas om en viss grupp av personer och inhämtandet inte tydligt fokuseras på en eller flera enskilda personer i Finland ska en anmälan enligt 46 § inte behöva göras. Om användningen av metoden riktas mot en viss grupp av personer i Finland och en person i gruppen känns igen i den meningen att dennes identitet kan fastställas, ska 46 § om underrättelse om användning av metoder för underrättelseinhämtning tillämpas på anmälan om att metoden används på samma sätt som om den systematiska observationen skulle riktas mot en person.

På samma sätt som i fråga om andra metoder för underrättelseinhämtning ska det också beslutet om systematisk observation ange de fakta som informationsinhämtningen om en person eller grupp grundar sig på för att den som fattar beslut om användningen har möjlighet till grundlig beslutsprövning. När underrättelsemyndigheten själv fattar beslutet är det som anges i beslutet av stor betydelse både för den interna kontrollen och för att möjliggöra underrättelseombudsmannens tillsyn.

10 §. *Beslut om förtäckt inhämtande av information vid civil underrättelseinhämtning.* Enligt 1 mom. är det chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning som ska besluta om förtäckt inhämtande av information vid civil underrättelseinhämtning.

Kravet på förtrogenhet för den polisman som hör till befälet vid skyddspolisen beror på att det är särskilt viktigt att inse var gränsen går mellan förtäckt inhämtande av information och täckoperationer. När någon är förtrogen med metoderna minskar risken för att det avslöjas att informationsinhämtning pågår samtidigt som verksamheten kan bli mer resultatrik. Dessa synpunkter är ännu mer framträdande när det gäller täckoperationer och bevisprovokation genom köp.

Enligt det föreslagna 2 mom. ska beslutet om förtäckt inhämtande av information fattas skriftligen. I beslutet ska följande nämnas: 1) åtgärden och dess syfte tillräckligt specificerat, 2) den verksamhet som avses i 3 §, 3) den person eller grupp av personer som åtgärden riktas mot, 4) de fakta som förutsättningarna för och inriktningen av det förtäckta inhämtandet av information grundar sig på, 5) den polisman som tillhör befälet vid skyddspolisen och som leder och övervakar utförandet av inhämtandet, 6) den planerade tidpunkten för genomförandet av åtgärden och 7) eventuella begränsningar och villkor för det förtäckta inhämtandet av information.

Med åtgärd avses den faktiska åtgärden för att inhämta informationen, såsom att vara taxiförare i syfte att transportera en person från ett ställe till ett annat. När det gäller användning av befogenheten förutsätts det uttryckligen att det utses en polisman som ansvarar bland annat för att åtgärden inte de facto är en täckoperation och att den som opererar under täckmantel och är taxiförare inte börjar skapa ett förtroligt förhållande till den transporterade, såsom täckoperationer förutsätter.

Vid förtäckt inhämtande av information behöver inte tidpunkterna för inledande och avslutande av inhämtandet anges med exakta klockslag eftersom det oftast är fråga om att utföra en enskild åtgärd vid en tidpunkt som inte anges i förväg.

Beslutsfattaren (chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning) kan i fråga om förtäckt inhämtande av information fastställa begränsningar och uppställa villkor, liksom vid användning av andra metoder för underrättelseinhämtning. Begränsningarna kan bero t.ex. på proportionalitetsprincipen och på ändamålsenlighets-, rättssäkerhets- och arbetarskyddssynpunkter.

Enligt 3 mom. ska beslutet vid förändrade omständigheter vid behov ses över. Det är fullt möjligt att objektet för informationsinhämtningen framträder klarare under operationen och då ska användningen av metoden riktas mot den person eller grupp av personer som det ursprungligen var meningen att skaffa information om. Detta ålägger den för åtgärden ansvarige polismannen att följa att förutsättningarna för förtäckt inhämtande av information föreligger

och behovet av informationshämtning i synnerhet när den tidsmässiga skillnaden är stor mellan beslutet och genomförandet av informationshämtningen.

Om åtgärden inte tål uppskov, behöver ett beslut som avses i 1 mom. enligt det föreslagna 4 mom. inte upprättas i skriftlig form före det förtäckta inhämtandet av information. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter det att åtgärden har vidtagits.

Den bestämmelsen är ny i förhållande till 5 kap. 16 §. Skyddspolisen kan när situationen kräver det skyndsamt börja genomföra förtäckt inhämtande av information. Detta undanröjer inte kravet på ett skriftligt beslut, men ger möjlighet att tillämpa metoden i brådskande lägen. Beslut om förtäckt inhämtande av information ska göras skriftligen så fort det bara är möjligt. I brådskande lägen måste man se till att den som utför åtgärden är muntligen informerad om de uppgifter som med tanke på dennes arbetarskydd och rättssäkerhet ska skrivas in i beslutet.

11 §. *Beslut om teknisk avlyssning vid civil underrättelseinhämtning.* Enligt 1 mom. ska beslut om teknisk avlyssning som riktas mot en frihetsberövad person vid civil underrättelseinhämtning fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om teknisk avlyssning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.

Med en person som berövats sin frihet avses en häktad, anhållen eller på annan laglig grund gripen person som berövats sin frihet. För avlyssning krävs inte att den avlyssnade befinner sig i en cell, avtjänar straff i en straffanstalt, är isolerad i en tvångsinrättning, är häktad eller befinner sig i polisens förvaringslokaler. Det är onödigt att nämna dessa förutsättningar eftersom en frihetsberövad person i praktiken bara kan avlyssnas i utrymmen som han eller hon har tillstånd att besöka eller vistas i.

I fråga om brådskande beslut kan det hänvisas till det som framförs i motiveringen till 7 § 1 mom. Brådskande beslut måste vara möjliga på grund av den operativa verksamhetens natur. Det kan plötsligt uppkomma lägen där man inte hinner inhämta tillstånd av domstolen utan att väsentliga uppgifter för skyddet av den nationella säkerheten går förlorade. Ett sådant akut läge kan uppkomma exempelvis i samband med att någon radikaliseras under fängelsevistelse. I sådana fall ska samtalet mellan en eller flera fångar och deras besökare kunna bandas in utan eget deltagande.

Enligt 2 mom. ska beslut om annan teknisk avlyssning än den som avses i 2 mom. fattas av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning.

Tillstånd kan ges och beslut fattas för högst sex månader åt gången, föreskrivs det i 3 mom. I detta avseende är det som framförs i motiveringen till 6 § 2 mom. relevant.

I 4 mom. föreslås bestämmelser om vad som ska nämnas i yrkanden och beslut om teknisk avlyssning. I detta avseende är det som framförs i motiveringen till 6 § 3 mom. och 9 § 3 mom. huvudsakligen relevant.

Teknisk avlyssning ska enligt den föreslagna 2 punkten också kunna riktas mot ett utrymme eller någon annan plats. Med utrymme avses en plats som avgränsas av väggar och tak eller motsvarande konstruktioner. Ett utrymme särskiljs således konstruktionsmässigt från en plats, som i sin tur kan avse en allmän eller enskild plats. Med annan plats avses en plats utanför ett

utrymme som avgränsas av väggar och tak eller motsvarande konstruktioner, såsom exempelvis gårdsområden utanför affärsfastigheter.

Syftet med teknisk avlyssning ska enbart vara att skaffa information om verksamhet som allvarligt hotar den nationella säkerheten. Den här metoden kan ändå inriktas bredare än vad befogenheterna att bekämpa brottlighet tillåter, dvs. mot en person, en grupp av personer, ett utrymme och en annan plats, och denna mer tillåtande förutsättning leder att också andra än de personer som är relevanta med avseende på den civila underrättelseinhämtningen oundvikligen blir föremål för avlyssningen. Denna konstellation uppvägs av underrättelseombudsmannens rättsliga tillsyn över skyddspolisen. Avsikten med denna avlyssning av utrymmen är att få information om de personer som befinner sig där och om deras inbördes kontakter, men sådan avlyssning kan med avseende på nationell säkerhet också vara relevant när man vill ta reda på att ett visst utrymme inte används.

När den tekniska avlyssningen gäller någon annan plats än ett utrymme ska det i tillståndet och beslutet så exakt som möjligt anges hut stort det geografiska område är som den tekniska avlyssningen avses gälla. Området för teknisk avlyssning ska i möjligaste mån avgränsas så att det är så litet som bara möjligt.

Vid teknisk avlyssning ska gränsdragningen mellan utrymmen som används för stadigvarande boende och andra platser göras från fall till fall. Den polisman som yrkar tillstånd och som hör till befälet vid skyddspolisen eller beslutar om användning av teknisk avlyssning måste göra en bedömning av och vid behov ta reda på hur det förhåller sig. Om utrymmet eller platsen används för stadigvarande boende får denna metod inte användas. Denna princip kan frångås om en utredning visar att motsatsen gäller. Exempelvis kan en lokal som används som kontor de facto användas för boende (t.ex. HD 2009:54) och även motsatt förhållande kan råda.

12 §. *Beslut om optisk observation vid civil underrättelseinhämtning.* Enligt 1 mom. ska beslut om optisk observation som riktas mot en frihetsberövad person vid civil underrättelseinhämtning fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om optisk observation till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas. I detta avseende är det som framförs i motiveringen till 11 § 1 mom. relevant. Om en polisman som hör till befälet vid skyddspolisen i ett brådskande läge har beslutat om sådan observation och om domstolen anser att det inte fanns förutsättningar för ett sådant beslut måste användningen av den metoden avslutas och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas (46 §). Information som fåtts på detta sätt får dock användas på samma villkor som information får användas enligt 44 § 1 mom.

Enligt 2 mom. är det en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning som ska besluta om annan optisk observation än den som avses i 1 mom. I detta avseende är det som framförs i motiveringen till 11 § 2 mom. relevant.

Tillstånd kan ges och beslut fattas för högst sex månader åt gången, föreskrivs det i 3 mom. I detta avseende är det som framförs i motiveringen till 11 § 3 mom. relevant.

I 4 mom. föreslås bestämmelser om innehållet i yrkanden och beslut om optisk observation och de motsvarar bestämmelserna i 11 § 4 mom.

13 §. *Beslut om teknisk spårning vid civil underrättelseinhämtning.* Enligt 1 mom. ska beslut om teknisk spårning som riktas mot en person fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om spårning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.

Om en polisman som hör till befälet vid skyddspolisen i ett brådskande läge har beslutat om sådan spårning och om domstolen anser att det inte fanns förutsättningar för ett sådant beslut måste användningen av den metoden avslutas och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas (46 §). Information som fåtts på detta sätt får dock användas på samma villkor som information får användas enligt 44 § 1, 2 och 3 mom.

Enligt 2 mom. är det en polisman som hör till befälet vid skyddspolisen som ska besluta om annan teknisk spårning än den som avses i 1 mom. Detta motsvarar i fråga om beslutsnivå 5 kap. 22 § 2 mom. med undantag för brådskande beslut.

Tillstånd kan ges och beslut fattas för högst sex månader åt gången, föreskrivs det i 3 mom. Bestämmelsen motsvarar 5 kap. 22 § 3 mom.

I 4 mom. föreslås bestämmelser om vad som ska nämnas i yrkanden och beslut om teknisk spårning och de motsvarar huvudsakligen bestämmelserna om vad som ska nämnas i yrkanden och beslut om andra metoder för underrättelseinhämtning. Enligt 2 punkten ska det i yrkanden och beslut i förekommande fall också nämnas det föremål, det ämne eller den egendom som den tekniska spårningen riktas mot.

14 §. *Beslut om teknisk observation av utrustning vid civil underrättelseinhämtning.* Med teknisk observation av utrustning avses enligt 5 kap. 23 § 1 mom. att en funktion, informationsinnehållet eller identifieringsuppgifterna i en dator eller i en liknande teknisk anordning eller i dess programvara på något annat sätt än enbart genom sinnesförnimmelser observeras, upptas eller behandlas på något annat sätt för att utreda omständigheter som är av betydelse för förebyggande av ett brott. Vid civil underrättelseinhämtning är det inte fråga om att ”utreda omständigheter som är av betydelse för förebyggande av ett brott” utan om att inhämta information om sådan i 3 § avsedd verksamhet som kan antas hota den nationella säkerheten. Genom teknisk observation av utrustning får information om innehållet i ett meddelande eller om identifieringsuppgifter som avses i (5 kap.) 8 § inte inhämtas, sägs det i 2 mom i samma paragraf. Med identifieringsuppgifter avses enligt den bestämmelsen uppgifter som kan förknippas med en abonnent eller användare och behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.

Enligt 1 mom. ska beslut om teknisk observation av utrustning vid civil underrättelseinhämtning fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en polisman som hör till befälet vid skyddspolisen besluta om sådan observation till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.

Om en polisman som hör till befälet vid skyddspolisen i ett brådskande läge har beslutat om sådan observation och om domstolen anser att det inte fanns förutsättningar för ett sådant beslut måste användningen av den metoden avslutas och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas (46 §). Information som fåtts på detta sätt får dock användas på samma villkor som information får användas enligt 44 § 1, 2 och 3 mom.

Tillstånd kan ges för högst sex månader åt gången, föreskrivs det i 2 mom. I detta avseende är det som framförs i motiveringen till 6 § 2 mom. relevant. I 3 mom. föreslås bestämmelser om innehållet i yrkandet och beslutet på samma sätt som i fråga om andra metoder för underrättelseinhämtning.

15 §. *Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning vid civil underrättelseinhämtning.* Enligt det föreslagna 1 mom. får skyddspolisen vid civil underrättelseinhämtning inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning med en teknisk anordning. Ett villkor för inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning ska vara den allmänna förutsättningen enligt 4 § 1 mom. att man med den berörda metoden för underrättelseinhämtning med fog kan antas få information om sådan verksamhet enligt 3 § som allvarligt kan antas hota den nationella säkerheten.

I 2 mom. föreslås det bestämmelser om kommunikationsverkets kontrollbefogenhet. Det ska med tekniska metoder och övervakningsmetoder säkerställas att anordningen inte på grund av sina egenskaper orsakar skadliga störningar i det allmänna kommunikationsnätets anordningar eller tjänster. I praktiken kommer det att vara tillåtet att orsaka smärre och kortvariga störningar, men anordningen ska ändå inte få långvarig eller mer än ringa störning. Det har rent konkret uppdagats att en teknisk anordning som används för inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning kan orsaka andra anordningar i närheten kortvariga och smärre störningar.

Det är inte ändamålsenligt att inom civil underrättelseinhämtning inskränka den avsedda tekniska anordningen funktionaliteter till enbart identifiering av teleadresser och teleterminalutrustning. Detta hänger i synnerhet samman med teleavlyssning och teleövervakning inom ramen för underrättelseinhämtning som avser utländska förhållanden.

Enligt 3 mom. är det en polisman som hör till befälet vid skyddspolisen som ska besluta om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning.

Det finns i fråga om inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning inte någon motsvarande förteckning över det som ska nämnas i yrkanden och beslut om sådant inhämtande som det finns för andra metoder för underrättelseinhämtning. Däremot måste användningen av metoden dokumenteras tillräckligt exakt. Av ett beslut att använda metoden ska åtminstone följande framgå: de allmänna förutsättningarna för användning av metoden, den tjänsteman som fattat beslut om inhämtandet, beslutsdatum, beslutets giltighetstid och eventuella övriga villkor för beslutet.

16 §. *Installation och avinstallation av anordningar, metoder eller programvara vid civil underrättelseinhämtning.* Enligt 1 mom. ska en tjänsteman som är anställd vid skyddspolisen vid civil underrättelseinhämtning ha rätt att placera en anordning, metod eller programvara som används för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, optisk observation, teknisk spårning eller teknisk observation av utrustning på eller i föremål, ämnen, egendom, utrymmen, platser eller informationssystem som åtgärden riktas mot, om det behövs för att använda metoden. För att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran har tjänstemannen som är anställd vid skyddspolisen då rätt att i hemlighet ta sig in i ett sådant utrymme eller på en sådan plats eller i ett sådant informationssystem och att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemens säkerhetssystem.

Motsvarande bestämmelse finns i 5 kap. 26 § 1 mom. En skillnad är dock att begreppet polisman inte används, utan i stället talar man om en tjänsteman som är anställd vid skyddspolisen. På detta sätt öppnar man för möjligheten att installationen och avinstallationen kan utföras

även av någon annan tjänsteman än en polistjänsteman. Allt eftersom tekniken utvecklas kan användningen av metoder för underrättelseinhämtning kräva att en teknisk expert används för installation och avinstallation av anordningar, metoder eller programvara. Exempelvis måste man tillfälligt kunna kringgå, låsa upp eller passera vissa objekt eller informationssystem.

I det föreslagna 2 mom. sägs det att anordningar, metoder och programvara som används för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, optisk observation, teknisk spårning eller teknisk observation av utrustning får installeras i utrymmen som används för stadigvarande boende endast om domstolen har gett tillstånd till det på yrkande av en polisman som hör till befälet vid skyddspolisen.

Om det är en domstol som beslutar om användning av metoden för underrättelseinhämtning ska det också tillståndet att använda metoden också särskilt innehålla lov att installera anordningen, metoden eller programvaran. Däremot ska det inte krävas lov till att avinstallera den. Om det är en polisman som hör till befälet vid skyddspolisen eller en polisman inom skyddspolisen som beslutar om användning av metoden kan beslutet ange de behövliga uppgifterna om installation och avinstallation av anordningen, metoden eller programvaran. Polismän som hör till befälet vid skyddspolisen är chefen för skyddspolisen, biträdande chefer för skyddspolisen och avdelningschefer, polisjurister, överinspektörer och inspektörer vid skyddspolisen.

Installation och avinstallation av anordningar, metoder eller programvara ska vara en subsidiär befogenhetsregel som medger användningen av den egentliga metoden för underrättelseinhämtning. Detta utesluter inte skyldigheten att ansöka om tillstånd för exempelvis teleavlyssning eller teleövervakning.

En tjänsteman som är anställd vid skyddspolisen har rätt att i hemlighet ta sig in i ett utrymme eller någon annan plats eller i ett informationssystem för att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran. Dessutom får objektets eller informationssystemets säkerhetssystem tillfälligt kringgås, låsas upp eller passeras. Systemet får också tillfälligt störas. Befogenheten ger ändå inte rätt till husrannsakan som meddelas i efterskott. Det ligger i underrättelseverksamhetens natur att det kan uppkomma situationer där installationen av anordningen, metoden eller programvaran kräver intrång i det hemfridsskyddade området. Exempelvis kan en anordning eller programvara vid teknisk observation av utrustning behöva installeras i utrymmen som används för stadigvarande boende för en teknisk anordning.

Bestämmelsen tar inte ställning till hur tidigt anordningen, metoden eller programvaran får installeras eller hur sent den får avinstalleras, utan detta måste tillämparen själv bestämma. Det är inte acceptabelt att exempelvis objektet för teknisk observation är utrustat för sådan observation för all framtid. Då avses uttryckligen anordningar som skyddspolisen installerat, dvs. utanför tillämpningsområdet ligger de egenskaper som i sig finns i den tekniska anordningen och som möjliggör sådan observation. I detta avseende är det för att förhindra att användningen av metoden för underrättelseinhämtning avslöjas ändå viktigt att inte bestämma fasta tidsgränser, utan att bestämmelsen ger handlingsutrymme. Det är möjligt att den eller de personer som är föremål för metoden har sådan beredskap eller är så pass medvetna att någon möjlighet att installera, börja använda eller avinstallera anordningen, metoden eller programvaran inte finns när behovet uppstår utan först när tillfälle erbjuds.

När anordningar, metoder eller programvara installeras eller avinstalleras bör man alltid väga in den eventuella risken för att åka fast och även den möjliga risk som finns för att objektet för installationen skadas. Programvara finns det alltid en risk för ett informationssystems funktion när programvara installeras till systemet, och dessutom kan programvaran försvaga dess säkerhet. Således ska skyddspolisens åtgärder inte få orsaka större skada eller olägenhet än vad

som är nödvändigt i samband med att anordningar, metoder eller programvara installeras eller avinstalleras.

17 §. *Framställning om och plan för en täckoperation vid civil underrättelseinhämtning.* I paragrafen föreslås bestämmelser om täckoperationer inom civil underrättelseinhämtning.

Med en täckoperation avses enligt 5 kap. 28 § 1 mom. planmässigt inhämtande av information om en viss person eller dennes verksamhet genom infiltration, där falska, vilseledande eller förtäckta uppgifter eller registeranteckningar används eller falska handlingar framställs eller används för att förvärva förtroende som behövs för inhämtandet av information eller för att förhindra att inhämtandet av information avslöjas.

Skillnaden i förhållande till sådana täckoperationer som avses i 5 kap. 28 § 1 mom. avses vara dels villkoren för användning, dels också att inhämtande av information genom täckoperation om verksamhet som allvarligt hotar den nationella säkerheten också ska kunna riktas mot en grupp av personer. I detta avseende är det som framförs i motiveringen till 9 § 3 mom. relevant.

Infiltration ska också få gälla en sådan grupp av personer om vars bakomliggande verksamhet det är meningen att skaffa information. Det kan vara fråga om en grupp av personer eller en organisation som styr eller påverkar den grupp som är föremål för metoden, såsom exempelvis en utländsk underrättelsetjänsts verksamhet som siktar på hybridpåverkan av Finland genom att skada landets internationella relationer, ekonomiska intressen eller andra vitala intressen. Ett exempel på sådan verksamhet är omfattande styrning av immigranter till Finland.

Det ska inte krävas att den person eller grupp av personer som är föremål för metoden namnges eller specificeras genom att ange fysiska egenskaper, utan det räcker med att personen eller gruppen anges specifikt exempelvis genom sin verksamhet

Enligt 1 mom. ska följande nämnas i en framställning om en täckoperation: 1) den som föreslagit åtgärden, 2) den person eller grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information, 3) den verksamhet som avses i 3 §, 4) de fakta som förutsättningarna för och inriktningen av täckoperationen grundar sig på, 5) syftet med täckoperationen, 6) behovet av täckoperationen och 7) övriga uppgifter som behövs för att bedöma förutsättningarna för täckoperationen. Momentet motsvarar 5 kap. 31 § 2 mom.

Enligt 2 mom. ska en sådan skriftlig plan göras upp över genomförandet av en täckoperation som innehåller väsentlig och tillräckligt detaljerad information för beslutsfattandet om och genomförandet av täckoperationen. Vid förändrade omständigheter ska planen vid behov ses över.

Skyldigheten att se över planen innebär en skyldighet att kontinuerligt följa täckoperationen. Paragrafen räknar synnerligen detaljerat upp de uppgifter som behövs för utarbetande av en plan och som beslutsunderlag. Planen ska innehålla väsentlig och tillräckligt detaljerad information för beslutsfattandet om och genomförandet av täckoperationen. Den ska också kunna inbegripa en plan för avveckling av operationen, om det över huvud taget låter sig göras när man planerar att inleda en täckoperation. När planen är uppgjord blir det aktuellt att fatta beslut om täckoperationen.

18 §. *Beslut om en täckoperation vid civil underrättelseinhämtning.* Enligt 1 mom. ska beslut om en sådan täckoperation som avses i 17 § fattas av chefen för skyddspolisen. Beslut om täckoperationer som genomförs uteslutande i datanät får fattas också av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användning-

en av metoder för underrättelseinhämtning. Bestämmelsen motsvarar i huvudsak 5 kap. 32 § 1 mom.

Beslut om en täckoperation kan meddelas för högst sex månader åt gången, föreskrivs det i det föreslagna 2 mom. Bestämmelsen motsvarar 5 kap. 32 § 2 mom.

Enligt det föreslagna 3 mom. ska beslut om en täckoperation fattas skriftligen. I beslutet ska följande nämnas: 1) den som föreslagit åtgärden, 2) den polisman som ansvarar för genomförandet av täckoperationen, 3) identifikationsuppgifterna för de polismän som genomför täckoperationen, 4) den verksamhet som avses i 3 §, 5) den person eller grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information, 6) de fakta som förutsättningarna för och inriktningen av täckoperationen grundar sig på, 7) täckoperationens syfte och genomförandeplan, 8) tillståndets giltighetstid och 9) eventuella begränsningar och villkor för täckoperationen. Bestämmelsen motsvarar i huvudsak 5 kap. 32 § 3 mom.

Enligt 4 mom. ska beslutet vid förändrade omständigheter vid behov ses över. Beslut om avslutande av en täckoperation ska fattas skriftligen. Bestämmelsen motsvarar 5 kap. 32 § 4 mom.

Det behövs inga bestämmelser i 5 a kap. om domstolens avgörande om förutsättningarna för en täckoperation. För det första är det en stark presumtion när täckoperationer används som metod för underrättelseinhämtning att den erhållna informationen inte kommer att användas i en straffprocess. Även om detta ändå kan ske under ytterst exceptionella omständigheter är en domstolsgranskning av förutsättningarna för täckoperationer inte i motsvarande mån nödvändig som när det gäller 5 kap. i polislagen eller 10 kap. i tvångsmedelslagen, eftersom underrättelseombudsmannen utövar tillsyn över civil underrättelseinhämtning och användningen av metoder för underrättelseinhämtning.

19 §. *Brottsförbud vid civil underrättelseinhämtning.* I det föreslagna 1 mom. skrivs för klarhets skull den princip explicit ut som säger att en polisman vid skyddspolisen som företar en täckoperation vid civil underrättelseinhämtning inte får begå brott eller ta initiativ till ett brott. Också sådana initiativ som inte når upp till sådan anstiftan till brott som avses i strafflagen ska vara förbjudna för den som deltar i en täckoperation.

I 2 mom. finns bestämmelser om vissa situationer där en polisman går fri från straffansvar för förseelser. Om en sådan polisman vid skyddspolisen som företar en täckoperation begår en trafikförseelse, en ordningsförseelse eller något annat jämförbart brott för vilket det föreskrivna straffet är ordningsbot, går polismannen fri från straffansvar, om gärningen har behövts för att syftet med täckoperationen ska nås eller för att inhämtandet av information inte ska avslöjas.

Det rör i den meningen om en allmänt hållen bestämmelse att polismannen automatiskt kan befrias från straffansvar när han eller hon gör sig skyldig till förseelse som nämns i paragrafen. lagen innehåller flera bestämmelser utifrån vilka en polisman har rätt att handla på ett sådant sätt som utan uttrycklig befogenhetsbestämmelse skulle anses vara ett lagstridigt förfarande. Exempelvis har en polisman, en tullman, en gränsbevakningsman och en tjänsteman som avses i lagen om militär disciplin och brottsbekämpning inom försvarsmakten i ett uppdrag för att förebygga och avslöja brott enligt 48 § 5 mom. i vägtrafiklagen (267/1981) i observationsuppgifter och vid tekniska observationsuppgifter och en polisman i täckoperationsuppgifter och uppgifter som har samband med bevisprovokation genom köp enligt den bestämmelsen samma rätt som en förare av en polisbil som avger föreskrivna ljus- och ljudsignaler att med iakttagande av särskild försiktighet avvika från bestämmelserna i den lagen.

Det kan bli aktuellt med befrielse från ansvar bara när det slås fast att gärningen har behövts för att syftet med täckoperationen ska nås eller för att inhämtandet av information inte ska avslöjas. Med andra ord är befrielsen från straffansvar ytterst begränsad. I förhållande till 48 § 5 mom. i vägtrafiklagen blir den föreslagna bestämmelsen tillämplig exempelvis när en polisman som företar en täckoperation inte har iakttagit särskild försiktighet varvid inte heller det momentet är tillämpligt. Polismannen kan då gå fri från straffansvar med stöd av det föreslagna momentet.

I ett första skede är det underrättelseombudsmannen, som utövar tillsyn över underrättelseverksamheten, som ska granska den berörda polismannens förfarande.

20 §. *Beslut om bevisprovokation genom köp vid civil underrättelseinhämtning.* Med bevisprovokation genom köp avses enligt 5 kap. 35 § 1 mom. ett köpeanbud eller ett köp av ett föremål, ett ämne, egendom eller en tjänst som polisen gör för att förhindra ett brott i syfte att ta om hand eller påträffa ett föremål, ett ämne eller egendom som har samband med ett brott. Till skillnad från det som anges ovan föreslås det att syftet med bevisprovokation genom köp enligt denna paragraf ska vara att skaffa information om verksamhet som utgör ett allvarligt hot mot den nationella säkerheten. Det kan då vara fråga om bevisprovokation genom köp av exempelvis sådana produkter med dubbel användning som det inte är straffbart att inneha, men att det med tanke på den nationella säkerheten är nödvändigt att använda bevisprovokation genom köp.

Enligt 1 mom. i paragrafen fattar chefen för skyddspolisen beslut om bevisprovokation genom köp vid civil underrättelseinhämtning. Beslut om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten får fattas också av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning.

Enligt 2 mom. kan ett sådant beslut fattas för högst sex månader åt gången. I detta avseende kan hänvisas huvudsakligen till det som anförs i motiveringen till 5 § 2 mom.

Enligt 3 mom. i paragrafen ska beslut om bevisprovokation genom köp fattas skriftligen. I beslutet ska anges: 1) den åtgärd som avses i 3 §, 2) den person som är föremål för bevisprovokationen, 3) de fakta som förutsättningarna för bevisprovokationen grundar sig på, 4) de föremål, de ämnen, den egendom eller de tjänster som är föremål för bevisprovokationen, 5) syftet med bevisprovokationen, 6) beslutets giltighetstid, 7) den polisman som tillhör befälet vid skyddspolisen och som leder och övervakar genomförandet av bevisprovokationen genom köp, 8) eventuella begränsningar och villkor för bevisprovokationen. Momentet överensstämmer i huvudsak med 5 kap. 36 § 2 mom.

De resultatförväntningar som ställs på bevisprovokationen (3 punkten) är knutna till kravet på sannolikhet. Enligt 4 § 2 mom. i kapitlet får bevisprovokation genom köp användas bara om det med fog kan antas vara av synnerligen stor betydelse för att få information om verksamhet som allvarligt hotar den nationella säkerheten och bevisprovokationen är nödvändig för att få information om verksamhet som allvarligt hotar den nationella säkerheten.

Bevisprovokation genom köp kan också rikta sig till en person som så att säga agerar i god tro. En effektiv informationsinhämtning till exempel om terrorism förutsätter att skyddspolisen ska kunna få tillräckligt med information om terroristceller, betalningsförbindelser och handelsplatser samt om bakgrundsorganisationen och dess ledning. I en sådan situation kan det vara nödvändigt att rikta bevisprovokationen genom köp mot exempelvis en handelspartner till terroristcellen.

21 §. *Plan för genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning*. Enligt 1 mom. i paragrafen ska det över genomförandet av bevisprovokation genom köp *vid civil underrättelseinhämtning* upprättas en skriftlig plan, om detta behövs med hänsyn till operationens omfattning eller andra motsvarande skäl. Vid förändrade omständigheter ska enligt 2 mom. planen för genomförande av bevisprovokationen vid behov ses över.

Paragrafen motsvarar det som föreskrivs i 5 kap. 37 §. Det kan vara nödvändigt med en särskild plan över genomförandet av bevisprovokation genom köp i synnerhet för att avvärja de risker som ingår i verksamheten.

På grund av att bevisprovokation genom köp är en krävande åtgärd och till följd av de risker som är förknippade med underrättelseverksamhet blir det i praktiken aktuellt med en plan vid alla operationer. Det är möjligt att låta bli att upprätta en plan till exempel i samband med bevisprovokation genom köp som genomförs på grundval av en enkel tidningsannons eller av andra liknande orsaker.

Skyldigheten att se över planen innebär en fortlöpande skyldighet att följa upp bevisprovokationer genom köp. Det finns inte heller några hinder för att upprätta en plan för hur en bevisprovokation ska återkallas, om detta kan anses vara möjligt och nödvändigt när bevisprovokationen planeras.

22 §. *Beslut om genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning*. Enligt 1 mom. i paragrafen ska beslut om genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning fattas skriftligen. Beslutet ska fattas av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och är förtrogen med användningen av metoder för underrättelseinhämtning och som ansvarar för genomförandet av bevisprovokationen. Momentet överensstämmer med 5 kap. 37 § 1 mom.

Enligt 2 mom. ska följande nämnas i beslutet: 1) den polisman som beslutat om bevisprovokationen samt beslutets datum och innehåll, 2) identifikationsuppgifterna för de polismän som genomför bevisprovokationen, 3) hur det har säkerställts att bevisprovokationen inte får den som är föremål för åtgärden eller någon annan att begå ett brott som denne annars inte skulle begå, 4) eventuella begränsningar och villkor för bevisprovokationen. Momentet överensstämmer med 5 kap. 37 § 2 mom.

Om åtgärden inte tål uppskov, behöver enligt 3 mom. ett beslut som avses i 2 mom. inte upprättas i skriftlig form före bevisprovokationen. Efter bevisprovokationen ska beslutet dock utan dröjsmål upprättas i skriftlig form. Momentet överensstämmer med 5 kap. 37 § 3 mom.

Vid förändrade omständigheter ska enligt 4 mom. beslutet om genomförande av bevisprovokationen vid behov ses över. Momentet överensstämmer med 5 kap. 37 § 4 mom.

Syftet med en mångfaldig dokumentprocess är att försäkra sig om att en bevisprovokation kan genomföras korrekt. Dessutom har hela processen dokumenterats på ett tillförlitligt sätt med tanke på en eventuell utvärdering i efterhand. Framför allt på grund av de risker som är förenade med bevisprovokation genom köp kan det hända att man blir tvungen att utreda verksamheten ännu i efterhand.

23 §. *Säkerheten för polismän vid förtäckt inhämtande av information, täckoperationer, bevisprovokation genom köp och användning av informationskällor vid civil underrättelseinhämtning*. Enligt 1 mom. i paragrafen får en polisman som hör till befälet vid skyddspolisen besluta att en polisman som ska genomföra sådant förtäckt inhämtande av information, en sådan täckoperation eller sådan bevisprovokation genom köp eller förbereda eller genomföra så-

dan användning av informationskällor som avses i kapitlet förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att polismannens säkerhet ska kunna tryggas.

Momentet överensstämmer till en del med 5 kap. 39 § 1 mom. Momentet gäller så kallad säkerhetsavlyssning och säkerhetsobservation. Det föreslås att det till momentet fogas att den som förbereder eller genomför användningen av informationskällor också ska kunna förses med en teknisk anordning som möjliggör avlyssning och observation.

Med förberedelser för användningen av informationskällor avses åtminstone att en polisman vid skyddspolisen ska undersöka om en person som polisen har för avsikt att rekrytera som informationskälla har de personliga egenskaper som lämpar sig för någon som anlitas som informationskälla. Polismannen vid skyddspolisen kan i samband med användningen av informationskällor riskera sitt liv och sin hälsa på samma sätt som vid exempelvis täckoperationer. Detta gäller i synnerhet situationer då man ännu inte med säkerhet kan säga hur den som ska rekryteras som informationskälla kommer att förhålla sig till att en polisman som närmar sig honom eller henne. Det bör vara motiverat att skydda polismannen vid skyddspolisen för att trygga hans eller hennes säkerhet.

Enligt 2 mom. i paragrafen ska det vara tillåtet att uppta avlyssningen och observationen. Upptagningarna ska utplånas så snart de inte behövs för att trygga polismannens säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har samband med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller avskrivits.

Momentet överensstämmer i sak 5 kap. 39 § 2 mom. Enligt momentet ska bevarandet och utnyttjandet av upptagningar från säkerhetsavlyssningar och säkerhetsobservationer begränsas. Dessa får inte bevaras och användas för andra ändamål än för dem som nämns i bestämmelsen. Det kan i dessa fall vara fråga om till exempel att en polisman har utsatts för våld eller varit tvungen att använda våld eller att någon har skadats i samband med förtäckt informationsinhämtning, täckoperation eller bevisprovokation genom köp. I dessa fall kan upptagningarna behövas vid behandlingen av brottmålet eller skadeståndsärendet (RP 224/2010 rd, s. 129).

24 §. *Beslut om styrd användning av informationskällor vid civil underrättelseinhämtning.* Enligt 1 mom. i paragrafen är det chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning som ska besluta om styrd användning av informationskällor vid civil underrättelseinhämtning.

Med användning av informationskällor avses enligt 5 kap. 40 § 1 mom. annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av i 1 kap. 1 § i polislagen avsedda uppgifter av personer som inte hör till polisen eller till någon annan förundersökningsmyndighet (informationskälla). Enligt 40 § 2 mom. i kapitlet får polisen be att en för ändamålet godkänd informationskälla som har lämpliga personliga egenskaper och är registrerad samt har samtyckt till inhämtandet av information ska inhämta uppgifter som avses i 1 mom. (styrd användning av informationskälla). Enligt 3 mom. i paragrafen får vid styrd användning av informationskällor en informationskälla inte ombes inhämta uppgifter på ett sätt som förutsätter utövande av myndighetsbefogenheter eller äventyrar informationskällans eller någon annans liv eller hälsa. Innan en styrd användning av informationskälla inleds ska informationskällan upplysas om sina rättigheter och skyldigheter och i synnerhet om vad som är tillåten och förbjuden verksamhet enligt lagen. Informationskällans säkerhet ska vid behov tryggas under och efter inhämtandet av information.

Också vid civil inhämtning av underrättelser är det nödvändigt att i tillräcklig mån skydda informationskällans liv och hälsa under och efter inhämtningen av information. Om det finns skäl att misstänka att informationskällans säkerhet behöver skyddas redan före informationsinhämtningen eller att informationskällan behöver ett intensivare skydd, ska bestämmelsen om beslut om skyddande i 36 § tillämpas. Om skyddet av en informationskälla har inletts med stöd av 36 §, kan det också fortsätta med stöd av bestämmelsen i fråga.

Enligt 2 mom. i paragrafen kan ett beslut om styrd användning av informationskällor meddelas för högst sex månader åt gången. Momentet överensstämmer med bestämmelsen i 5 kap. 42 § 2 mom.

I 3 mom. i paragrafen ingår bestämmelser om kravet på att beslutet om styrd användning av informationskällor ska fattas skriftligen och om de uppgifter som ska anges i beslutet.

Vid förändrade omständigheter ska enligt 4 mom. beslutet vid behov ses över. Beslut om att styrd användning ska avslutas fattas skriftligen. Bestämmelserna överensstämmer med det som anges i 5 kap. 42 § 4 mom.

Enligt 5 mom. ska bestämmelser om registrering av informationskällor i ett personregister och betalning av arvode ingå i 5 kap. 41 §.

Utgångspunkten vid användningen av metoder för underrättelseinhämtning är att dessa i enlighet med 4 § 3 mom. inte får riktas mot utrymmen som används för stadigvarande boende. I förhållande till övriga befogenheter som gäller underrättelseverksamhet är situationen vid användning av informationskällor dock en annan, eftersom en polisman då inte själv utför informationsinhämtningen. Således har polismannen inte heller kontroll över informationskällans agerande. Vid styrd användning av en informationskälla kan en polisman vid skyddspolisen däremot i varje fall indirekt anses ha kontroll över informationskällan, eller åtminstone i den begäran om inhämtning av information som framförs till informationskällan bör det noteras att informationsinhämtningen inte förutsätter att man går in i utrymmen som används för stadigvarande boende. Därför ska den polisman som har kontakt med en informationskälla också informera informationskällan om de begränsningar som anges ovan. Det är dock, på samma sätt som vid täckoperationer, tillåtet för en informationskälla att gå in i ett utrymme som används för stadigvarande boende, om det är nödvändigt för att förhindra att användningen av informationskällan röjs.

25 §. *Tryggande av informationskällor vid civil underrättelseinhämtning.* Skyddspolisen är i princip skyldig att vid behov trygga informationskällans säkerhet under och efter inhämtningen av information. Informationskällans rätt till skydd ersätter dock inte det vittnesskyddsprogram som avses i lagen om vittnesskyddsprogram (88/2015). Om en informationskälla behöver skydd under en längre tid och det riktas ett allvarligt hot mot personens liv eller hälsa och hotet inte effektivt kan avvärjas med andra åtgärder, är det motiverat att för informationskällans del överväga att inleda ett vittnesskyddsprogram.

Enligt 1 mom. kan skyddspolisen med en informationskällas samtycke vid civil underrättelseinhämtning övervaka informationskällans bostad eller något annat utrymme som informationskällan använder för boende och dess omedelbara närmiljö med kamera eller någon annan teknisk anordning, metod eller programvara som placerats på platsen, om det behövs för att avvärja en fara som hotar informationskällans liv eller hälsa. Genom samtycket försäkrar man sig om att också informationskällan själv vill ha skydd. Utomstående behöver inte upplysas om att informationskällan skyddas.

Momentet gör det möjligt att i den bostad som används av en informationskälla som är i behov av skydd och i bostadens omedelbara närhet installera olika säkerhetssystem som är nödvändiga för att skydda informationskällan, såsom övervakningskameror, rörelsedetektorer och andra givare. Med andra utrymmen som en informationskälla använder för boende avses till exempel hotellrum.

I motsats till situationen vid teknisk avlyssning ska övervakning inte ske utan att den person som är föremål för åtgärden är medveten om det och inte heller i syfte att inhämta information. Däremot är syftet med övervakning att skydda informationskällan, men skyddet kan indirekt också vara förknippat med avsikten att inhämta information, exempelvis om vilka personer som rör sig i området.

Övervakning får inte utföras om det inte är nödvändigt för att avvärja ett hot mot informationskällans liv och hälsa. Med detta avses att informationskällans liv och hälsa är utsatt för åtminstone en potentiell fara.

Bestämmelsen ska också gälla fall då de anordningar som installerats i en skyddsbehövandes hem eller dess omedelbara närhet utsträcker sig till ett område som skyddas av någon annans hemfrid, även om det inte är dess kärnområde. En sådan situation kan förekomma i ett höghus där en övervakningskamera filmar också husbolagets invånares gemensamma trappuppgång eller i ett radhus där kameran filmar också gemensamma gårdsplaner.

Skyddet av informationskällor förutsätter att utomstående inte informeras om kameraövervakning och annan övervakning för att undvika risken för avslöjande och för att skydda informationskällans liv och hälsa.

Enligt 2 mom. i paragrafen ska övervakningen genast avslutas, om den inte längre behövs för att avvärja en fara som hotar informationskällans liv eller hälsa. Detta innebär att säkringsåtgärderna genast ska avslutas när det inte längre finns någon grund för att trygga informationskällans säkerhet.

Enligt 3 mom. ska upptagningar som uppkommit enligt 1 mom. utplånas så snart de inte behövs för att trygga informationskällans säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har att göra med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller avskrivits.

Upptagningarna får inte bevaras och användas för andra ändamål än de som nämns i bestämmelsen. Det kan i dessa fall vara fråga om till exempel att en informationskälla har utsatts för våld och myndigheten direkt ingriper i handlingen. Om det i en sådan situation väcks åtal mot myndigheten, kan de upptagningar som samlats in i samband med tryggandet av informationskällans säkerhet användas för att påvisa att den åtalade är oskyldig eller skyldig. I dessa fall kan upptagningarna behövas vid behandlingen av ett eventuellt brottmål eller skadeståndsärende. Ett brottmål eller ett skadeståndsärende kan dock kräva behandling bakom stängda dörrar.

Informationskällans rätt till skydd ersätter dock inte det vittnesskyddsprogram som avses i lagen om vittnesskyddsprogram. Om en informationskälla behöver skydd under en längre tid och det riktas ett allvarligt hot mot personens liv eller hälsa och hotet inte effektivt kan avvärjas med andra åtgärder, kan man överväga att inleda ett vittnesskyddsprogram för att skydda informationskällan.

I 4 mom. i paragrafen ingår bestämmelser om säkerhetsavlyssning och säkerhetsobservation. Inom civil underrättelseinhämtning är det nödvändigt att rekrytera från kärnan i verksamhet som utgör ett allvarligt hot mot den nationella säkerheten, vilket leder till att den som samtycker till att vara informationskälla kan utsätta sitt liv och sin hälsa för fara. Informationskällor har inte heller fått samma utbildning för användningen av våld som polismän som deltar i hemlig informationsinhämtning. Av det följer att tryggandet av deras säkerhet med myndighetsåtgärder får en mycket central ställning.

Informationskällor får bara kortvarigt utrustas med tekniska anordningar som möjliggör säkerhetsavlyssning eller säkerhetsobservation i situationer då det inte går att tillräckligt effektivt garantera informationskällans säkerhet med andra myndighetsåtgärder eller då det i det närmaste är omöjligt att trygga informationskällans säkerhet med andra åtgärder. Att en åtgärd är enskild innebär att den är begränsad till en enskild händelse som gäller informationsinhämtning. Att åtgärden är nödvändig är ett uttryck för att informationskällans säkerhet inte kan tryggas på något annat sätt.

Beslutsfattaren ska vara tillräckligt insatt i användningen av informationskällor. Ett uttryck för detta är bland annat att en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning ska besluta om åtgärden. Förutom på beslutet av polismannen i fråga ska säkerhetsavslyssningen och säkerhetsobservationen grunda sig på samtycke från informationskällan. En informationskälla ska ha sådana personliga egenskaper att hen kan agera naturligt även om hen bär en teknisk anordning som möjliggör säkerhetsavlyssning.

Syftet med åtgärden i fråga är bara att trygga informationskällans säkerhet. Således får den inte användas för att kringgå teknisk avlyssning och observation. Detta yttrar sig så att upptagningarna från avlyssningen och observationen ska utplånas utan dröjsmål när de inte längre behövs för att trygga informationskällans säkerhet.

I 5 mom. föreskrivs det om skydd av informationskällors liv och hälsa. När det gäller tryggande av informationskällor är det fråga om att temporärt skapa en förtäckt identitet för en informationskälla med hjälp av falska, vilseledande eller förtäckta uppgifter eller registeranteckningar, eller falska handlingar. I sådana situationer som avses i momentet är det i andra hand fråga om att trygga överlämnandet av de uppgifter som informationskällan innehar.

Förutsättningen för att en temporär förtäckt identitet ska få skapas är att åtgärden är nödvändig för att skydda informationskällans liv och hälsa.

Tryggande av informationskällor kan bli aktuellt till exempel om en informationskälla innehar särskilt viktiga uppgifter om verksamhet som allvarligt hotar den nationella säkerheten och uppgifterna inte kan överlämnas till skyddspolisen på annat sätt än genom ett personligt möte med informationskällan.

Med enskilt fall avses i bestämmelsen att skapandet av en temporär förtäckt identitet för en informationskälla alltid ska prövas från fall till fall.

Enligt den sista meningen i momentet ska en registeranteckning rättas när förutsättningarna enligt momentet inte längre finns. Detta betyder att när det inte längre är nödvändigt att trygga informationskällan med avseende på skyddet av informationskällans liv och hälsa ska uppgifterna om den förtäckta identiteten korrigeras och de falska handlingarna fråntas informationskällan. Informationskällan får inte använda sådana uppgifter och handlingar som avses i momentet för andra syften än för att skydda sitt eget liv och sin egen hälsa.

26 §. *Platsspecifik underrättelseinhämtning.* I paragrafen definieras begreppet platsspecifik underrättelseinhämtning.

Med platsspecifik underrättelseinhämtning avses underrättelseinhämtning på någon annan plats än en plats som används för stadigvarande boende eller en plats beträffande vilken det finns anledning att anta att underrättelseinhämtningen kommer att omfatta information som någon enligt 17 kap. 11, 13, 14, 16, 20, 21 eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om och som görs för att hitta föremål, egendom, handlingar, information eller omständigheter.

Befogenheten är ny. Den platsspecifika underrättelseinhämtningen ska i princip göras i hemlighet så att platsens ägare, innehavare eller någon annan person inte känner till att skyddspolisen är där. Också benämningen på metoden för underrättelseinhämtning, platsspecifik underrättelseinhämtning, är ett indirekt uttryck för detta.

Den platsspecifika underrättelseinhämtningen ska enligt definitionen inriktas på en plats, vilket även inbegriper utrymmen. Den kan å ena sidan inriktas på en plats som avses i 8 kap. 1 § 4 mom. i tvångsmedelslagen. Enligt bestämmelsen avses med *platsgenomsökning* genomsökning av andra platser än sådana som avses i 2 eller 3 mom. trots att de inte är allmänt tillgängliga eller den allmänna tillgängligheten har begränsats eller hindrats vid tidpunkten för genomsökningen, eller genomsökning av ett fordon.

Å andra sidan kan den platsspecifika underrättelseinhämtningen inriktas på sådana platser som skyddas av hemfrid enligt 24 kap. 11 § i strafflagen, men dock inte på utrymmen som används för stadigvarande boende. Föremål för platsgenomsökning kan således vara fritidsbostäder och andra utrymmen som är avsedda för boende, såsom hotellrum, tält, husvagnar och fartyg som kan bebos, trappuppgångar i bostadshus samt gårdar som utgör de boendes privata område och de byggnader som är fast förbundna med sådana gårdar. Men om det visar sig att en plats eller ett utrymme ändå används för stadigvarande boende, får platsgenomsökningen inte inriktas på dem.

Platsspecifik underrättelseinhämtning får dock inte inriktas på en bostad som är skyddad av hemfrid enligt 24 kap. 11 § i strafflagen, om det inte är möjligt att visa att platsen verkligen används för något annat än stadigvarande boende (GrUU 36/1998 rd, KKO 2009:54).

Platsspecifik underrättelseinhämtning får inte heller inriktas på platser beträffande vilka det kan antas att underrättelseinhämtningen kommer att omfatta information som någon enligt 17 kap. 11, 13,14, 16, 20, 21 § eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om. Bland de platser som avses i bestämmelsen kan nämnas läkarmottagningar, advokatbyråer och juridiska byråer, mediehus och tidningsredaktioner, utrymmen avsedda för präster i sådana registrerade religionssamfund som avses religionsfrihetslagen (453/2003) och servercentraler som kan antas överföra information som omfattas av tystnadsplikt eller tystnadsrätt enligt bestämmelsen. Frågan om huruvida den platsspecifika underrättelseinhämtningen är godtagbar med tanke på de grundläggande fri- och rättigheterna bedöms närmare i avsnittet om lagstiftningsordning.

Den platsspecifika underrättelseinhämtningen kan inriktas till exempel på ett slutet fordon som inte används för stadigvarande boende. Som ett typexempel på platsspecifik underrättelseinhämtning kan nämnas en hemlig genomsökning av bilens bagageutrymme eller handskfack i syfte att finna ett föremål eller finna och kopiera en handling. Andra exempel på platser som den platsspecifika underrättelseinhämtningen kan inrikta sig på är hotellrum, tält, husvagnar och fartyg som kan bebos, samt trappuppgångar i bostadshus, affärer, ämbetsverk, kaféer eller rum i affärslokaler.

För att man ska kunna ta sig in i slutna lokaler eller utrymmen kan det i vissa fall krävas att hinder avlägsnas, till exempel att en låst dörr eller skåpdörr måste öppnas på ett sätt som är lämpligt i situationen i fråga.

Uttrycket ”plats” används som överbegrepp och omfattar utrymmen och andra platser. Med det sistnämnda avses närmast områden utomhus. Med ”utrymmen” avses platser som är avgränsade av väggar och ofta också av tak.

Syftet med platsspecifik underrättelseinhämtning är att hitta information som är av betydelse för den nationella säkerheten. Det är dock inte tillåtet att beslagta föremål, dokument eller annan egendom som finns i utrymmet, utan nödvändig information som gäller dessa ska lagras till exempelvis genom fotografering eller kopiering. Om ett föremål i utrymmet behöver kopieras, ska det göras med hjälp av en sådan teknisk anordning eller metod som inte kräver att föremålet tas i beslag.

Vid beslut som gäller platsspecifik underrättelseinhämtning ska särskild vikt fästas vid den princip som avses i 1 och 2 § om respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna, i synnerhet när man överväger att inrikta den platsspecifika underrättelseinhämtningen på områden som skyddas av hemfrid.

Bestämmelser om hur den som är föremål för underrättelseinhämtning samt ägaren eller innehavaren till platsen ska informeras om den platsspecifika underrättelseinhämtningen finns i 46 §.

27 §. *Beslut om platsspecifik underrättelseinhämtning vid civil underrättelseinhämtning.* I paragrafen ingår beslut om platsspecifik underrättelseinhämtning.

Om platsspecifik underrättelseinhämtning riktas mot någon annan hemfridsskyddad plats än en plats som används för stadigvarande boende eller en plats som allmänheten inte har tillträde till eller dit tillträdet för allmänheten har begränsats eller förhindrats under den tid den platsspecifika underrättelseinhämtningen genomförs, ska beslut om platsspecifik underrättelseinhämtning fattas av domstol på yrkande av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning. Av karaktären av befogenheten följer att skyddspolisen med stöd av ett beslut av domstol har rätt att ta sig in på en sluten plats utan att fästa avseende vid låsta dörrar eller andra låsta hinder eller handla på annat lämpligt sätt med beaktande av förhållandena.

Även om den platsspecifika underrättelseinhämtningen inte ingriper i kärnområdet för skyddet av hemfriden, är det på grund av den platsspecifika underrättelseinhämtningens hemliga karaktär i de fall som avses i 1 mom. motiverat att ge domstolen befogenhet att fatta beslut, eftersom man inom platsspecifik underrättelseinhämtning inte iakttar förfarandet vid husrannsakan. Den som är föremål för informationsinhämtning har då inte möjlighet att följa upp myndighetens agerande på samma sätt som vid exempelvis allmän husrannsakan eller platsgenomsökning.

Om det ärende som avses i 1 mom. inte tål uppskov, får enligt 2 mom. i paragrafen chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om platsspecifik underrättelseinhämtning till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.

I praktiken kommer beslut i brådskande fall att vara mycket ovanliga eftersom tvångsmedelsavdelningen vid Helsingfors tingsrätt, som fattar beslut om användningen av metoder för underrättelseinhämtning, har jour dygnet runt.

Om chefen för skyddspolisen eller en polisman som hör till befälet vid skyddspolisen i en brådskande situation har fattat ett beslut och domstolen anser att det inte finns förutsättningar för åtgärden, ska användningen av underrättelsemetoden upphöra och det material som metoden gett upphov till och de anteckningar som gäller informationen genast förstöras (46 §).

Enligt 3 mom. ska chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om annan platsspecifik underrättelseinhämtning än den som avses i 1 mom.

Momentet ska inbegripa sådana platser som är allmänt tillgängliga och i fråga om vilka den allmänna tillgängligheten inte har begränsats eller hindrats vid tidpunkten för åtgärden. Till momentets tillämpningsområde hör dessutom sådana fordon som inte används för stadigvarande boende

Enligt 4 mom. i paragrafen kan tillstånd ges och beslut fattas för högst en månad åt gången.

Platsspecifik underrättelseinhämtning är en metod för informationsinhämtning vars syfte är att finna information som är av betydelse för den nationella säkerheten. Utmärkande för metoden är att det uppstår ett behov av att besöka vissa platser mer än en gång. Sådana situationer motiverar tiden för tillståndet och beslutet om platsspecifik underrättelseinhämtning är inte en engångsföreteelse, även om det kunde vara det. Som exempel kan nämnas fall då det är nödvändigt att i samband med underrättelseinhämtningen kopiera viktiga dokument mer än en gång för att skydda den nationella säkerheten.

Enligt 5 mom. ska i ett yrkande och i ett beslut om platsspecifik underrättelseinhämtning tillräckligt noggrant specificeras: 1) den verksamhet som avses i 3 §, 2) den plats som är föremål för den platsspecifika underrättelseinhämtningen, 3) de fakta utifrån vilka det anses finnas förutsättningar för platsspecifik underrättelseinhämtning, 4) i den utsträckning det är möjligt vad som söks genom den platsspecifika underrättelseinhämtningen, 5) eventuella begränsningar i den platsspecifika underrättelseinhämtningen.

När sakens brådskande natur kräver det får enligt 6 mom. ett beslut om platsspecifik underrättelseinhämtning dokumenteras efter att den platsspecifika underrättelseinhämtningen har genomförts.

Om det vid platsspecifik underrättelseinhämtning visar sig att underrättelseinhämtningen har inriktats på sådan information som någon enligt 17 kap. 11, 13, 14, 16, 20, 21 § eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om, ska underrättelseinhämtningen till denna del genast avslutas och de anteckningar och kopior som gäller informationen genast förstöras.

Med uttrycket ”ska underrättelseinhämtningen till denna del genast avslutas” avses att den platsspecifika underrättelseinhämtningen i övrigt inte behöver avslutas, om inte syftet med användningen av platsspecifik underrättelseinhämtning annars har uppnåtts eller det inte längre finns förutsättningar för användningen.

28 §. *Kopiering vid civil underrättelseinhämtning*. Enligt paragrafen har skyddspolisen vid civil underrättelseinhämtning rätt att kopiera handlingar och föremål.

En handling eller ett föremål ska kopieras utan att det tas i beslag för att minimera risken för att den civila underrättelseoperationen röjs.

I praktiken kan en handling kopieras genom att man fotograferar den eller skannar den med hjälp av ett skanningsprogram i telefonen. Med kopiering av ett föremål avses till exempel en situation då det är nödvändigt att kopiera föremålet genom att använda en 3 D-skanner.

Kopieringen ska gälla fysiska dokument och föremål i realvärlden. Om informationen ingår i ett dokument som har lagrats i en teknisk anordning, ska uppgifterna i princip inhämtas med hjälp av teknisk observation av utrustningen. Genom att använda sig av kopieringsbefogenheter kan man också skriva av anteckningar från skärmen på en öppen dator. Om uppgifterna på skärmen inhämtas med hjälp av en teknisk anordning, såsom en kamera, är det fråga om teknisk observation av utrustning.

29 §. *Kopieringsförbud vid civil underrättelseinhämtning.* I paragrafen föreskrivs om kopieringsförbud.

Den information som inhämtas med hjälp av en metod för underrättelseinhämtning ska i princip inte användas som bevis i en straffprocess. Kopieringsförbudet har således inte motsvarande funktion inom underrättelseverksamheten som vid straffprocessuella beslag eller kopiering. Även av den anledningen är det inte ändamålsenligt att reglera kopieringsförbudet på samma sätt med motsvarande bestämmelser om förbud mot beslag, kopiering och bevisning. Däremot är det skyddsintresse som ligger bakom kopieringsförbudet detsamma.

Enligt 1 mom. i paragrafen får en handling eller något annat objekt som avses i 26 § inte kopieras vid civil underrättelseinhämtning om objektet innehåller sådant som någon enligt 17 kap. 11, 13, 14, 16, 20 eller 21 § i rättegångsbalken har skyldighet eller rätt att vägra vittna om. Kopieringsförbudet ska dock inte inbegripa det område som omfattas av 17 kap. 10 och 12 § i rättegångsbalken, eftersom skyddspolisen för att kunna fullgöra sin uppgift behöver få information som gäller statens säkerhet, Finlands förbindelser till en annan stat eller en internationell organisation eller information som faller under tystnadsplikten för tjänstemän.

Om tystnadsplikten eller tystnadsrätten grundar sig på 17 kap. 11 § 2 eller 3 mom. eller 13, 14, 16 eller 20 § i rättegångsbalken, är det enligt 2 mom. en förutsättning för förbudet utöver det som föreskrivs i 1 mom. dessutom att objektet innehas av en person som avses i bestämmelsen i fråga eller av någon som står i ett sådant förhållande till honom eller henne som avses i 22 § 2 mom. i det kapitlet, eller av den till vars förmån tystnadsplikten eller tystnadsrätten har föreskrivits.

Bestämmelsen motsvarar i detta avseende det kopieringsförbud som föreskrivs i 7 kap. 3 § 2 mom. i tvångsmedelslagen. Förbudet gäller bara om objektet innehas av en person som avses i momentet eller av den till vars förmån tystnadsplikten har föreskrivits. Att inneha objektet ska tolkas på samma sätt som i gällande lagstiftning. Innehavet inbegriper således också försändelser som levereras av posten, en kurir eller någon annan tredje part. På grund av underrättelseverksamhetens karaktär kommer bestämmelsen i fråga inte att tillämpas i någon större utsträckning.

Enligt 3 mom. gäller kopieringsförbudet dock inte, om 1) den som avses i 17 kap. 11 § 2 eller 3 mom., 13 § 1 eller 3 mom., 14 § 1 mom. eller 16 § 1 mom. i rättegångsbalken och till vars förmån tystnadsplikten har föreskrivits samtycker till kopiering, 2) en person som avses i 17 kap. 20 § 1 mom. i rättegångsbalken samtycker till kopiering.

30 §. Kopieringsförbud som gäller teleavlyssning, teleövervakning och basstationsuppgifter. Handlingar och data som innehas av ett i 3 § 27 punkten i lagen om tjänster inom elektronisk kommunikation avsett teleföretag *(teleföretag)* eller en i 36 punkten i den paragrafen avsedd sammanslutningsabonnent och som innehåller uppgifter om meddelanden som avses i 5 kap. 5 § 1 mom. i denna lag eller innehåller identifieringsuppgifter som avses i 5 kap. 8 § 1 mom. eller basstationsuppgifter som avses i 5 kap. 11 § 1 mom. får enligt 1 mom. inte kopieras.

Paragrafen anknyter till ändamålsbundenheten när det gäller användningen av metoderna för underrättelseinhämtning samt till att teleavlyssning, teleövervakning och inhämtande av mobilteleapparaters läge på grund av sin karaktär ingriper i de grundläggande fri- och rättigheterna, och därför är beslutströskeln för deras del högre än för kopiering. För tydlighetens skull är förbudet i paragrafen nödvändigt för att betona att man genom kopiering inte får kringgå användningen av metoder för underrättelseinhämtning från telenät och de strängare villkor som föreskrivs för användningen av dem.

31 §. *Kopiering av försändelser vid civil underrättelseinhämtning.* Enligt paragrafen ska skyddspolisen vid civil underrättelseinhämtning ha rätt att kopiera ett brev eller annan försändelse innan den anländer till mottagaren.

Brev inbegriper åtminstone en sådan brevförsändelse som avses i postlagen (415/2011). Med brevförsändelse avses en för befordran lämnad adresserad försändelse som väger högst två kilogram och som innehåller ett meddelande på ett fysiskt medium. Med annan försändelse avses *postpaket* dvs. en adresserad varuförsändelse som ingår i de samhällsomfattande tjänsterna och som har lämnats för transport. Med annan försändelse avses också en brevförsändelse som väger över två kilogram.

En brevförsändelse kan vara en underrättelse på vilket fysiskt medium som helst. Kopieringen av försändelser omfattar dock inte elektroniska meddelanden som kräver andra befogenheter för att kunna mottas. Med dessa kan jämföras meddelanden som sänds till exempel i digital form på ett usb-minne eller en cd-skiva. I förslaget föreskrivs således bara om fysiska postförsändelser, inte om meddelanden som förmedlas elektroniskt. Därför ska ett meddelande senast vid utdelningen vara i en fysisk form.

Till en försändelses egenskaper hör enligt definitionen att den lämnats för befordran exempelvis i ett kuvert eller som postkort. Brevförsändelser kan särskiljas från paketförsändelser utifrån i vilken form de vanligen skickas. Kuvertet kan vara ett traditionellt kuvert eller ett annat omslag, till exempel av plast.

I fråga om metoden kan det vid kopiering i viss mån vara fråga om en liknande åtgärd som i 7 kap. 5 § i tvångsmedelslagen (Beslag och kopiering av försändelser). Vid kopiering av försändelser inom den civila underrättelseinhämtningen är det dock fråga om att en försändelse kopieras i hemlighet för objektet. Bestämmelser om när den som varit föremål för inhämtning av information ska underrättas om detta finns i 47 §.

32 §. *Kvarhållande av försändelser för kopiering.* Om det finns skäl att anta att ett brev eller någon annan motsvarande försändelse som får kopieras vid civil underrättelseinhämtning kommer att anlända till eller redan finns vid ett verksamhetsställe för post, en järnvägsstation eller en del av en sådan eller ett verksamhetsställe som innehas av den som yrkesmässigt transporterar försändelser i samband med trafik eller annars, får enligt 1 mom. en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning förordna att försändelsen ska hållas kvar på verksamhetsstället i fråga tills kopiering hinner utföras.

Momentet överensstämmer till en del med regleringen i 7 kap. 6 § i tvångsmedelslagen. Beträffande godstrafiken är förutsättningen att det finns ett fast verksamhetsställe från vilket försändelsen kan avhämtas eller som ser till att försändelsen skickas till mottagaren. Ett sådant verksamhetsställe är till exempel kontoret för någon som bedriver företagsverksamhet i logistikbranschen och som därifrån sköter frågor som gäller inkommande frakt och håller kontakt med mottagarna.

Med ”verksamhetsstället” i slutet av momentet hänvisas till alla platser som anges i momentet, dvs. postkontoret, järnvägsstationen eller en del av det eller ett verksamhetsställe som innehas av den som yrkesmässigt transporterar försändelser i samband med trafik eller annars.

Enligt 2 mom. i paragrafen får det förordnande som avses i 1 mom. meddelas för högst en månad räknat från det att chefen för verksamhetsstället har fått kännedom om förordnandet. Försändelsen får inte utan tillåtelse av den tjänsteman som avses i 1 mom. överlämnas till någon annan än honom eller henne eller till den som han eller hon har utsett.

Det får inte utsättas en längre tidsfrist än en månad, eftersom personalen på verksamhetsstället genom föreläggandet åläggs ytterligare en skyldighet att övervaka ankommande försändelser. Efter att den tidigare tidsfristen har gått ut kan ett nytt föreläggande utfärdas.

Med verksamhetsställe hänvisas till de verksamhetsställen som avses i 1 mom.

Enligt 3 mom. ska chefen för verksamhetsstället genast meddela den som har utfärdat föreläggandet när försändelsen har anlänt. Denne ska utan ogrundat dröjsmål besluta om kopiering.

Om det inte har varit möjligt att närmare identifiera en ankommande försändelse och när den som utfärdat föreläggandet eller dennes företrädare anländer till verksamhetsstället är uppenbart att försändelsen inte får kopieras utifrån exempelvis avsändarens namn eller handstil på kuvertet, får den inte öppnas eller undersökas, utan ska utan dröjsmål skickas vidare.

33 §. *Beslut om kopiering.* Enligt 1 mom. i paragrafen ska en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om kopiering vid civil underrättelseinhämtning. Orsaken till kravet på förtrogenhet är att det är särskilt viktigt att kunna dra en gräns mellan kopiering och andra metoder för informationsinhämtning, såsom teknisk observation av utrustning. I dessa fall gäller i hög grad att kunna hantera kopieringsförbud. Också genom utbildning kan man minimera risken för att informationsinhämtningen röjs samt bidra till ett bra resultat.

Om ett ärende inte tål uppskov, får enligt 2 mom. i paragrafen också någon annan än en sådan polisman vid skyddspolisen som avses i 1 mom. i ett enskilt fall besluta om kopiering, till dess att den polisman som avses i 1 mom. har avgjort saken. Ärendet ska ges till den polisman som avses i 1 mom. för avgörande genast när det är möjligt, dock senast 24 timmar efter det att metoden för inhämtning av information började användas.

Vid civil underrättelseinhämtning kan det uppstå situationer då den för uppdraget förordnade polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning inte alltid deltar i den operativa verksamheten eller att den platsspecifika underrättelseinhämtningen måste utföras i sådana förhållanden att det inte är möjligt att hålla kontakt med den polisman vid skyddspolisen som hör till befälet. Till exempel i dessa fall är det nödvändigt att det finns möjlighet att fatta brådskande beslut. Behovet av att kopiera ett dokument i brådskande ordning kan också bero på att situationen är oväntad.

34 §. *Förstöring av kopior.* Enligt paragrafen ska en kopia utan dröjsmål förstöras om det framgår att det har kopierats sådant material som det är förbjudet att kopiera eller att informationen inte behövs för att skydda den nationella säkerheten.

Den situation som avses i paragrafen konkretiseras närmast då det första efter kopieringen visar sig att kopieringen har gällt en handling eller ett föremål som omfattas av kopieringsförbud. Sådan information måste förstöras och den får inte på något sätt användas. Skyldigheten att förstöra information gäller naturligtvis också situationer då man på basis av en analys redan har hunnit föra in uppgifter om kopian i skyddspolisens register.

Om material som omfattas av kopieringsförbud har kopierats är det motiverat att informera underrättelseombudsmannen om detta. Bestämmelser om när föremålet för informationsinhämtningen ska informeras om att en försändelse eller ett meddelande har kopierats finns i 47 § 1 mom.

En kopia ska genast förstöras också om det visar sig att den inte har någon betydelse för skyddet av den nationella säkerheten.

Det ska antecknas när en kopia har förstörts.

35 §. *Förfarandet i domstol i ärenden som gäller civil underrättelseinhämtning.* I paragrafen sammanställs de viktigaste bestämmelserna om behandling i domstol av metoder för underrättelseinhämtning. Bestämmelserna ska också tillämpas på den underrättelseinhämtning som avser datatrafik i lagen om civil underrättelseinhämtning avseende datatrafik.

Enligt 1 mom. i paragrafen ska ett tillståndsärende som gäller en metod för civil underrättelseinhämtning handläggas av Helsingfors tingsrätt. Tingsrätten är domför med ordföranden ensam. Sammanträdet kan hållas även vid en annan tidpunkt och på en annan plats än vad som förskrivs om en allmän underrätts sammanträde. Underrättelseombudsmannens rätt att närvara vid behandlingen av tillståndsärenden regleras i en kommande lag om övervakning av underrättelseverksamheten.

Bestämmelsen om domstolens beslutföra sammansättning och om tiden och platsen för sammanträdet överensstämmer i sak med bestämmelsen i 3 kap. 1 § 2 mom. i tvångsmedelslagen om den myndighet som fattar häktningsbeslut.

Enligt 2 mom. i paragrafen ska ett yrkande om användning av en metod för underrättelseinhämtning göras skriftligen. För ett yrkande om användning av en metod för underrättelseinhämtning gäller således samma krav på skriftlig form som i 3 kap. 3 § 1 mom. i tvångsmedelslagen.

I momentet föreskrivs dessutom att ett yrkande som gäller användningen av en metod för underrättelseinhämtning utan dröjsmål ska tas upp till behandling i domstol i närvaro av den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman som är insatt i ärendet. Kravet på behandling utan dröjsmål förutsätter att ett anhängigt ärende som gäller en metod för underrättelseinhämtning så snabbt som möjligt delas ut till de domare som fattar beslut i ärendet och att det fastställs en tidpunkt för det sammanträde som behandlar ärendet. Det förutsätts att den förordnade tjänstemannen är så förtrogen med metoderna för underrättelseinhämtning att han eller hon kan besvara frågor och motivera yrkandet.

I 3 mom. ska ärendet avgöras skyndsamt. Om det inte ställs krav på att domstolen behandlar ärendet skyndsamt kan användningen av metoderna för underrättelseinhämtning förlora sin betydelse och i värsta fall leda till att den nationella säkerheten äventyras.

Enligt momentet kan behandlingen också ske med anlitande av videokonferens eller någon annan lämplig teknisk dataöverföring där de som deltar i behandlingen har sådan kontakt att de kan tala med och se varandra. Metoderna för överföring av data i samband med behandlingen kommer då att vara desamma som vid hemligt inhämtande av information med stöd av 5 kap. 45 § 2 mom. och i samband med hemliga tvångsmedel enligt 10 kap. 43 § 2 mom. i tvångsmedelslagen. I takt med utvecklingen av tekniken och krypteringsmetoderna inom datatrafiken kan det också vara möjligt att behandlingen sker via videokonferens eller någon annan lämplig teknisk dataöverföring. Detta är dock inte en förpliktande bestämmelse och vid behandlingen ska alltid iakttas vad som föreskrivs i 7 mom.

Innehållet i beslutet om en metod för underrättelseinhämtning ska enligt 4 mom. i paragrafen föreskrivas separat för varje metod för underrättelseinhämtning. Genom bestämmelsen om innehållet i beslutet uppmärksammas domstolen på att den i sitt beslut om användning av en metod för underrättelseinhämtning ska ange de omständigheter som föreskrivs i detalj i 6–8 §, 11–14 § och 27 § i detta kapitel.

I sin bedömning av dessa omständigheter stöder sig domstolen enbart på de uppgifter som skyddspolisen uppgett för domstolen. Därför är det av yttersta vikt att det av motiveringen till såväl tillståndsyrkandet som tillståndet framgår de omständigheter som lett till ansökan om och beviljandet av tillstånd och den rättsliga slutledningen. Även om skyddspolisen arbetar under tjänstemannaansvar, framhåller en behandling som baserar sig på ett enpartsförhållande betydelsen av att domaren aktivt utövar sin frågerätt och fullgör sin utredningsskyldighet.

Enligt momentet ska beslutet meddelas omedelbart eller senast när behandlingen av ärenden som gäller metoder för underrättelseinhämtning, vilka anknyter till samma underrättelsehelhet, har avslutats. Bestämmelsen förutsätter att domstolen när det handlar om beslut i ärenden som gäller metoder för underrättelseinhämtning agerar på samma sätt som när ett häktningsbeslut meddelas med stöd av 3 kap. 10 § 1 mom. i tvångsmedelslagen.

Om domstolen har beviljat tillstånd till teleavlyssning eller teleövervakning, får den enligt 5 mom. i paragrafen pröva och avgöra ett ärende som gäller beviljande av tillstånd i fråga om en ny person, teleadress eller teleterminalutrustning utan att den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman är närvarande, om det har förflutit mindre än sex månader från den muntliga förhandlingen av det tidigare tillståndsärendet. Ärendet kan behandlas utan att tjänstemannen är närvarande också om användningen av metoden för underrättelseinhämtning redan har avslutats.

För att skyddspolisens och domstolens resurser ska kunna utnyttjas ändamålsenligt och effektivt föreslås det att ärenden som gäller byte av teleadress eller teleterminalutrustning inte i alla situationer ska behöva behandlas i sammanträde. Det förenklade förfarande som avses i momentet kan tillämpas enligt domstolens prövning och bara om tillståndet fortfarande är i kraft. Tillståndsärendet ska således behandlas minst en gång per halvår, i närvaro av den tjänsteman som svarar för framställandet av yrkandet. En förutsättning för förenklat förfarande är dessutom att det är fråga om en och samma person och om samma verksamhet som allvarligt hotar den nationella säkerheten och som ligger till grund för användningen av metoden för underrättelseinhämtning som i det tidigare beviljade tillståndet.

Fallen enligt den andra meningen i momentet är förenade med samma slags ändamålsenlighetsaspekter som de situationer som avses i den första meningen. Den andra meningen ska således gälla fall då chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och är förtrogen med användningen av metoder för underrättelseinhämtning har fattat ett temporärt beslut om användningen av metod för underrättelseinhämtning med stöd av 7 § 1 mom., 11 § 1 mom., 12 § 1 mom., 13 § 1 mom. eller 27 § 2 mom. samt

fall då en polisman som hör till befälet vid skyddspolisen har fattat ett temporärt beslut om användningen av metod för underrättelseinhämtning med stöd av 8 § 1 mom. eller 14 § 1 mom.

Enligt 6 mom. i paragrafen får ett beslut i ett tillståndsärende inte överklagas genom besvär. Klagan mot beslutet får anföras utan tidsfrist vid Helsingfors hovrätt. Klagan ska behandlas skyndsamt.

Regleringen överensstämmer till denna del med 5 kap. 45 § 5 mom. med preciseringen att Helsingfors hovrätt anges som domstol för klagan.

I 7 mom. i paragrafen föreskrivs att det vid handläggningen av ett ärende som gäller en metod för underrättelseinhämtning ska fästas särskild vikt vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.

Ett ärende kan vid behov behandlas någon annanstans än vid domstol, till exempel i skyddspolisens lokaler. Särskild vikt ska fästas vid att sekretessen iakttas och informationssäkerheten tryggas. De viktigaste bestämmelserna om sekretess finns i lagen om offentlighet vid rättegång i allmänna domstolar (370/2007).

36 §. *Skyddande av civil underrättelseinhämtning.* I paragrafen föreskrivs om skyddet för inhämtning av information på samma sätt som i 5 kap. 46 § 2 och 3 mom. I 5 a kap. är det inte nödvändigt att föreskriva om den rätt till fördröjning med att ingripa som avses 46 § 1 mom. i fråga, eftersom skyldigheten för en polisman vid skyddspolisen att ingripa eller agera ingår i 15 c § 3 mom. i polisförvaltningslagen och i bestämmelserna i 44 § i detta kapitel.

I 15 c § 3 mom. i polisförvaltningslagen är det fråga om så kallad tjänstgöringsskyldighet som åligger varje polisman. Det har också ställts vissa villkor för en polismans tjänstgöringsskyldighet, såsom brådska och nödvändighet. Att förhindra ett allvarligt brott och inleda en utredning kan innebära bara en anmälan till polisenheten i regionen. I skyldigheten ingår åtminstone de minimiåtgärder som nödvändigtvis måste vidtas för att uppnå det resultat som avses i bestämmelsen. För en polisman är det alltså möjligt att fullgöra sin tjänstgöringsskyldighet exempelvis genom att göra en anmälan till larmcentralen och uppge nödvändiga uppgifter. I det sammanhanget är det inte nödvändigt att uppge sådana uppgifter som kan leda till att en civil underrättelseinhämtning röjs eller riskera säkerheten i arbetet. Till exempel om situationen kräver det kan anmälan göras under förtäckt identitet eller också anonymt.

Begreppet allvarligt brott i 15 c § 3 mom. i lagen i fråga är beroende i första hand av situationen i sin helhet, men också av den person som är föremål för brott och personens möjligheter att försvara sig. Om brottet gäller ett litet barn eller en person som på grund av sjukdom, ålder eller annan orsak är försvarslös, har personen få möjligheter att försvara sig, vilket förutsätter en större tjänstgöringsskyldighet av den polisman som sköter den civila underrättelseinhämtningen än om brottet skulle rikta sig mot en vuxen person som kan försvara sig själv. Det är alltid fråga om övervägning från fall till fall.

Bestämmelsen i 44 § i detta kapitel (Utlämnande av information för brottsbekämpning) kommer att vara en specialbestämmelse jämfört med 15 c § 3 mom. i polisförvaltningslagen, eftersom den med tanke på tjänstgöringsskyldigheten ger en kvalificerad skyldighet att ingripa i sådana brott för vilka det föreskrivna strängaste straffet är fängelse i minst sex år (44 § 1 och 2 mom.). Detta gäller utan undantag situationer då en polis inom skyddspolisen utövar sin tjänst, eftersom det i 44 § avses fall då det i samband med användningen av en metod för underrättelseinhämtning framgår sådan information som kan användas för att förhindra ett allvarligt brott

eller som är av stor betydelse för utredningen av ett brott. De fall som avses i 15 c § 3 mom. i polisförvaltningslagen innefattar också situationer utanför tjänstgöringen på polisens fritid.

En polismans tjänstgöringsskyldighet som föreskrivs i 15 c § 3 mom. i polisförvaltningslagen och regleringen i 44 § står inte i strid med varandra, även om det i bestämmelserna när det gäller förhindrandet av allvarliga brott dock finns en viss överlappning. Att överlämna information för att bekämpa brott handlar om att överlämna information som är nödvändig för att förhindra eller utreda brott, så att den behöriga myndigheten kan vidta behövliga åtgärder. Anmälningsskyldigheten eller anmälningsrätten ska dock grunda sig på de uppgifter som inhämtats i samband med användningen av en metod för underrättelseinhämtning, medan polismannens tjänstgöringsskyldighet är oberoende av tid, plats och huruvida polismannen utövar sin tjänst eller inte. När det gäller brott som upptäcks i samband med användningen av olika metoder för underrättelseinhämtning fullgörs polismannens tjänstgöringsskyldighet i princip genom en anmälan enligt 44 §. Om en polisman som utför civil underrättelseinhämtning, förutsatt att den operativa säkerheten och säkerheten i arbetet gör det möjligt, personligen kan ingripa för att förhindra ett allvarligt brott, utgör regleringen i 44 § inget hinder.

Enligt 1 mom. i paragrafen får skyddspolisen använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt upprätta och använda falska handlingar, om det är nödvändigt för att skydda den civila underrättelseinhämtningen.

Skyddet gäller bara tjänstemän. Uttrycket ”för att skydda den civila underrättelseinhämtningen” omfattar förutom redan genomförd, pågående och framtida användning av metoder för underrättelseinhämtning också annan verksamhet som anknyter till civil underrättelseinhämtning. Detta innebär bland annat att en för ett civilt underrättelseinhämtningsuppdrag förordnad tjänsteman kan använda falska eller vilseledande personuppgifter så länge det är nödvändigt för skötseln av uppdraget. Det är dock inte möjligt att med stöd av momentet skapa en ny identitet för en informationskälla eller en utomstående. På grund av olika anknytande problem och orsaker relaterade till rättssäkerheten får man inte ta alltför lätt på skyddet. Exempelvis användningen av falska handlingar leder till felaktiga registeranteckningar i myndighetens register. Med falska registeranteckningar och falska handlingar avses uttryckligen myndighetens handlingar och register. Skyddet är därför nödvändigt.

Enligt 2 mom. ska en registeranteckning som avses i 1 mom. rättas när förutsättningarna enligt det momentet inte längre finns. En registeranteckning ska således rättas när förutsättningarna enligt momentet inte längre finns, dvs. skyddet inte längre behövs eller det inte längre är nödvändigt. Den föreslagna regleringen överensstämmer i detta avseende i sak med 5 kap. 46 § 3 mom.

37 §. *Beslut om skyddande*. Enligt 1 mom. i paragrafen ska beslut om registeranteckningar och upprättande av handlingar enligt 36 § 1 mom. fattas av chefen för skyddspolisen. Bestämmelsen om fattandet av beslut överensstämmer med bestämmelsen i 5 kap. 47 § 1 mom.

Enligt 2 mom. ska en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om annat än i 1 mom. avsett skyddande.

Enligt 3 kap. 19 § i statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information ska chefen för skyddspolisen förordna en anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information att svara för användningen av vilseledande eller förtäckta registeranteckningar och falska handlingar.

Enligt 3 mom. ska den myndighet som har fattat beslut om registeranteckningar och upprättande av handlingar föra en förteckning över anteckningarna och handlingarna, övervaka användningen av dem samt se till att anteckningarna rättas.

Bestämmelsen överensstämmer i sak med 5 kap. 47 § 3 mom. De åtgärder som anges i 36 § 1 mom. får inte inriktas på den förteckning som avses i momentet.

38 §. *Yppandeförbud vid civil underrättelseinhämtning.* Enligt första meningen i 1 mom. i paragrafen får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning förbjuda en utomstående att röja sådana omständigheter om användningen av en metod för civil underrättelseinhämtning som denne fått kännedom om, om det är motiverat för att skydda användningen av metoden för underrättelseinhämtning.

Grunden för användning av en metod för underrättelseinhämtning är alltid en verksamhet som är föremål för civil underrättelseinhämtning och utgör ett allvarligt hot mot den nationella säkerheten. Vid användningen av en metod för underrättelseinhämtning finns det risk för att hamna i en situation där utomstående hjälp är nödvändig eller rentav oundviklig. Till exempel vid platsspecifik underrättelseinhämtning kan det vara nödvändigt att begära tjänster av det bolag som svarar för skötseln av bostadsaktiebolaget. På detta sätt kan utomstående få tillgång till information som, om den röjs, kan äventyra åtminstone användningen av den aktuella metoden för underrättelseinhämtning, men samtidigt utgöra ett hot mot den nationella säkerheten. Avsikten är att minimera risken för att metoden för underrättelseinhämtning avslöjas och samtidigt skydda också sådana taktiska och tekniska metoder som bör hållas hemliga och i sista hand den nationella säkerheten.

Enligt andra meningen i 1 mom. förutsätts det dessutom att den utomstående med anledning av sitt uppdrag eller sin ställning har bistått eller blivit ombedd att bistå vid användningen av en metod för underrättelseinhämtning. Därför kan vem som helst inte åläggas yppandeförbud, till exempel invånarna i ett bostadsaktiebolag eller andra utomstående, som av en händelse upptäcker installationen av en anordning för teknisk observation.

I bestämmelsen har uttrycket användning av en metod för underrättelseinhämtning en vidare betydelse och inbegriper bland annat civil underrättelseinhämtning samt skyddet av de metoder för underrättelseinhämtning som används vid militär underrättelseinhämtning då skyddspolisen och en myndighet för militär underrättelseinhämtning samarbetar. Det är motiverat att meddela yppandeförbud åtminstone då det finns risk för att användningen av en metod för underrättelseinhämtning röjs om inte en utomstående beläggs med förbud.

Enligt 2 mom. i paragrafen meddelas ett yppandeförbud för högst ett år åt gången. Förbudet ska ges i skriftlig form och bevisligen delges den som förbudet gäller. I förbudet ska det specificeras de omständigheter som förbudet omfattar, nämnas förbudets giltighetstid och anges hotet om straff för överträdelse av förbudet. Regleringen i momentet överensstämmer med 5 kap. 48 § 2 mom.

I 3 mom. föreskrivs om förbud mot att överklaga ett beslut om yppandeförbud. Enligt bestämmelsen får ändring i ett beslut om yppandeförbud inte sökas genom besvär. Den som belagts med förbud får dock överklaga beslutet utan tidsfrist. Klagan ska behandlas i brådskande ordning.

Underrättelseombudsmannen ska enligt 61 § 2 mom. alltid delges ett beslut om yppandeförbud.

I ett yppandeförbud ska ingå uppgifter om den bestämmelse med stöd av vilken besvär inte är möjliga. Ett besvärsförbud är inte något hinder för den som belagts med yppandeförbud att delge underrättelseombudsmannen om att ett yppandeförbud har meddelats.

Förbudet mot att överklaga ett yppandeförbud behandlas nedan under rubriken Förhållande till grundlagen samt lagstiftningsordning.

Enligt 4 mom. i paragrafen ska till straff för överträdelse av yppandeförbudet dömas enligt 38 kap. 1 eller 2 § i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans i lag. Regleringen i momentet överensstämmer med 5 kap. 48 § 3 mom.

I 5 mom. föreskrivs om rätten för den som belagts med yppandeförbud att, trots bestämmelsen i 4 mom., informera underrättelseombudsmannen om yppandeförbudet. Detta är motiverat med tanke på rättssäkerheten för den som belagts med yppandeförbud. På detta sätt får var och en som är föremål för yppandeförbud trots yppandeförbudet möjlighet att informera underrättelseombudsmannen om sin syn på förbudet.

Med tanke på rättssäkerheten för den som belagts med yppandeförbud är det viktigt att personen också underrättas om möjligheten att meddela underrättelseombudsmannen om förbudet och begära att ombudsmannen vidtar åtgärder eller att anföra en i lagen avsedd klagan hos hovrätten. Detta hänför sig till myndighetens skyldigheter i ett förvaltningsärende.

39 §. *Beslut om användning av metoder för underrättelseinhämtning i vissa fall.* Enligt 1 mom. i paragrafen ska beslut om civil underrättelseinhämtning och användning av metoder för underrättelseinhämtning utanför Finland fattas av chefen för skyddspolisen.

Med andra ord ska chefen för skyddspolisen fatta ett beslut på operativ nivå om civil underrättelseinhämtning utomlands och om de metoder för underrättelseinhämtning som ska användas i samband med det. Eftersom underrättelseinhämtning som avser utländska förhållanden kan vara känslig är det viktigt att man i besluten beaktar de prioriteter som fastställts för informationsinhämtningen samt regleringen i 58 § och de riktlinjer som utfärdats med stöd av den.

Enligt 2 mom. tillämpas i fråga om innehållet i framställningar, planer, yrkanden och beslut som gäller användningen av metoder för underrättelseinhämtning vad som i kapitlet föreskrivs om framställningar, planer, yrkanden och beslut samt tillstånd.

I beslut som gäller användningen av metoder för underrättelseinhämtning någon annanstans än i Finland ska motsvarande uppgifter anges som i framställningar, planer, yrkanden eller beslut när en metod för underrättelseinhämtning används i Finland.

Enligt 3 mom. i paragrafen får bestämmelserna i 4 § 4 mom., 16 § 3 mom., 41, 44, 46 och 47 § i detta kapitel tillämpas på sådan civil underrättelseinhämtning och användning av metoder för underrättelseinhämtning som avses i 1 mom.

Skyddspolisens prövningsrätt samt användningen av metoder för underrättelseinhämtning också inom underrättelseinhämtning som avser utländska förhållanden styrs av polisrättsliga principer vars betydelse inom civil underrättelseinhämtning behandlas närmare i motiveringen till 2 §. I synnerhet betydelsen av principen om respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna spelar en viktig roll inom underrättelseinhämtning som avser utländska förhållanden. Inom underrättelseinhämtningen som avser utländska förhållanden kan bestämmelserna i Europakonventionen i viss mån utgöra en tolkningsgrund framför allt i sådana fall då territorialstatens rättssystem, kultur och förhållanden inte överensstämmer med det västerländska systemet. Inom underrättelseverksamhet som avser utländska förhål-

landen kan argument som utgår från de mänskliga rättigheterna användas som ett hjälpmedel som styr tolkningen.

Av 2 § 3 mom. och 22 § i grundlagen följer att finländska tjänstemän inte heller när de befinner sig utomlands får handla på ett sätt som kränker de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. Eftersom underrättelseinhämtning som avser utländska förhållanden kan vara känslig är det dock i enskilda fall motiverat att inte alltid nödvändigtvis tillämpa de bestämmelser som särskilt anges i momentet. Ett uttryck för detta är formuleringen ”kan … tillämpas”. Detta ger chefen för skyddspolisen rätt att bedöma när bestämmelserna kan tillämpas eller när det inte är motiverat att tillämpa dem.

I 4 § 4 mom. i kapitlet föreskrivs om förbudet mot att rikta användningen av metoder för underrättelseinhämtning mot utrymmen som används för stadigvarande boende. Utgångspunkten är att man inte heller inom underrättelseinhämtning som avser utländska förhållanden får rikta användningen av metoder för underrättelseinhämtning mot någons bostad. Gränsdragningen inom underrättelseinhämtningen som avser utländska förhållanden kan vara så gott som omöjlig åtminstone då underrättelseinhämtningen görs i mindre utvecklade eller underutvecklade länder där det till följd av infrastrukturen inte är möjligt att fastställa bostäders användningsändamål utifrån myndigheternas register.

Utgångspunkten är att installationer som avses i 16 § inte ska göras i sådana utrymmen som omfattas av bestämmelsen i 3 mom. i paragrafen. Vid underrättelseinhämtning som avser utländska förhållanden är det dock nödvändigt att komma åt att göra installationer för att det ska vara möjligt att genomföra underrättelseinhämtningen, exempelvis i servercentraler där anslutningar möjliggör teleavlyssning och teleövervakning.

I 29 § i kapitlet föreskrivs om kopieringsförbud och i 41 § om förbud mot avlyssning och observation, vilka också efter prövning ska tillämpas inom underrättelseverksamhet som avser utländska förhållanden.

I 46 § i kapitlet ingår en bestämmelse om utplåning av information som fåtts i en brådskande situation. Bestämmelsen i fråga ska inte tillämpas inom underrättelseinhämtning som avser utländska förhållanden, eftersom chefen för skyddspolisen utan undantag beslutar om användningen av varje metod för underrättelseinhämtning.

I 47 § i kapitlet föreskrivs om underrättelse om användningen av metoder för underrättelseinhämtning. I 1 mom. i paragrafen föreskrivs om skyldigheten att utan dröjsmål skriftligen underrätta den som varit föremål för de metoder för underrättelseinhämtning som anges där efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts. Om den som varit föremål för underrättelseinhämtning i samband med underrättelseinhämtning som avser utländska förhållanden underrättas om användningen en metod för underrättelseinhämtning, avslöjas det att underrättelseverksamhet utövats på en annan stats territorium, vilket kan skada förhållandena mellan staterna. Detta talar för att föremålet för underrättelseinhämtningen inte ska underrättas med beaktande av att en finsk domstol inte är behörig att besluta om uppskov med underrättelsen eller helt och hållet underlåta att underrätta om att en metod för underrättelseinhämtning har använts inom underrättelseinhämtning som avser utländska förhållanden, eftersom den inte heller är behörig att besluta om användningen av metoden för underrättelseinhämtning. Det är således helt och hållet skyddspolisens uppgift att besluta om prövningen av beslutet.

40 §. *Beräkning av tidsfrister vid civil underrättelseinhämtning.* Enligt 1 mom. i paragrafen ska vid beräkning av tidsfrister enligt detta kapitel inte lagen om beräknande av laga tid (150/1930) tillämpas.

Enligt 2 mom. löper en i månader uttryckt tid ut den dag i månaden som till sitt ordningsnummer motsvarar den dag då tidsfristen började löpa. Om motsvarande dag inte finns i den månad då den bestämda tiden löper ut, löper den bestämda tiden ut på månadens sista dag.

Paragrafen överensstämmer i sak med 5 kap. 49 § i gällande lag.

41 §. *Förbud mot avlyssning och observation vid civil underrättelseinhämtning.* Enligt 1 mom. får teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation inte riktas mot sådan kommunikation, som parterna i kommunikationen inte får vittna om med stöd av 17 kap. 13, 14, 16, 20 § eller 22 § 2 mom. i rättegångsbalken.

I 17 kap. 13 § i rättegångsbalken föreskrivs om att ett rättegångsombud, ett rättegångsbiträde eller en tolk inte olovligen får vittna om vad han eller hon har fått veta vid skötseln av ett uppdrag i anslutning till en rättegång, vid lämnande av juridisk rådgivning som gäller huvudmannens rättsliga ställning vid förundersökning eller i någon annan handläggningsfas inför en rättegång och vid lämnande av juridisk rådgivning som gäller inledande eller undvikande av rättegång. I paragrafen föreskrivs dessutom att en advokat, ett rättegångsbiträde som avses i lagen om rättegångsbiträden med tillstånd eller ett offentligt rättsbiträde inte får olovligen vittna om en enskild persons eller en familjs hemlighet eller affärs- eller yrkeshemligheter som han eller hon har fått kännedom om i något annat uppdrag än ett sådant som avses ovan. I 17 kap. 14 § i rättegångsbalken föreskrivs att en läkare eller någon annan yrkesutbildad person inom hälso- och sjukvården inte får vittna om känsliga uppgifter om en enskild persons eller familjs hälsotillstånd eller någon annan hemlighet som gäller en enskild person eller familj och som han eller hon har fått kännedom om på grund av sin ställning eller uppgift, om inte den till vars förmån tystnadsplikten har föreskrivits ger sitt samtycke till det. I 17 kap. 16 § i rättegångsbalken förskrivs att en präst eller någon annan person i motsvarande ställning inte får vittna om vad han eller hon har fått veta under bikt eller enskild själavård, om inte den till vars förmån tystnadsplikten har föreskrivits ger sitt samtycke till det. När ett meddelande enligt lagen om yttrandefrihet i masskommunikation har gjorts tillgängligt för allmänheten, får meddelandets upphovsman, utgivaren och utövaren av programverksamheten enligt 17 kap. 20 § vägra vittna om vem som har lämnat de upplysningar som meddelandet grundar sig på samt om upphovsmannens identitet. 17 kap. 22 § 2 mom. i rättegångsbalken utvidgar det personliga tillämpningsområdet för vissa förbud mot att vittna och rätten att vägra vittna som anges ovan. Enligt bestämmelsen i fråga har en person som har fått information som avses i 11 § 2 eller 3 mom., 13 § 1 eller 3 mom., 14 § 1 mom. eller 20 § 1 mom. när han eller hon var anställd hos eller annars biträdde den som avses i bestämmelsen i fråga motsvarande skyldighet eller rätt att vägra vittna som de som avses i de nämnda bestämmelserna. Hänvisningen i 22 § 2 mom. till 11 § 2 och 3 mom. i rättegångsbalken lämpar sig inte här, eftersom det här inte föreslås någon bestämmelse om förbud mot avlyssning och observation såsom det uttryckligen görs i 11 § i rättegångsbalken. Enligt förslaget ska en bestämmelse om anknytande förbud mot underrättelseinhämtning ingå i 12 § i lagen om civil underrättelseinhämtning avseende datatrafik.

De metoder för underrättelseinhämtning som avses i 1 mom. får inte heller installeras (16 §) för användning på platser där det kan antas att information som avses i 1 mom. kan bli föremål för underrättelseinhämtning och som någon enligt momentet har skyldighet eller rätt att vägra vittna om och denna skyldighet eller rätt enligt Finlands grundlag omfattas av skyddet av grundläggande fri- och rättigheter. Sådana platser är till exempel läkarmottagningar, advokatbyråer och juridiska byråer, mediehus och tidningsredaktioner, utrymmen avsedda för präster i sådana registrerade religionssamfund som avses religionsfrihetslagen (453/2003) och servercentraler som kan antas överföra information som omfattas av tystnadsplikt eller tystnadsrätt enligt bestämmelsen.

Om det under tiden för teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation eller vid något annat tillfälle framkommer att det är fråga om ett meddelande som inte får avlyssnas eller observeras, ska åtgärden enligt 2 mom. i paragrafen avbrytas och de upptagningar som fåtts genom åtgärden och anteckningarna om de uppgifter som fåtts genom den genast utplånas. Skyldigheten att genast utplåna uppgifterna kompletterar bestämmelsen om att iaktta förbudet mot avlyssning och observation. Om det i samband med informationsinhämtningen framgår att det förbud mot inriktning av metoderna för underrättelseinhämtning som avses i 1 mom. har kränkts, ska skyldigheten att utplåna upptagningar och anteckningar enligt 2 mom. iakttas genast när det framgår att meddelandet omfattas av förbud mot underrättelseinhämtning.

Enligt 3 mom. gäller de förbud mot avlyssning och observation som avses i denna paragraf dock inte sådana fall där en i 1 mom. avsedd person deltar i verksamhet som är föremål för civil underrättelseinhämtning och det också för hans eller hennes del har fattats beslut om teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation. I det moment som det nu är fråga om är det tillåtet att avvika från det förbud mot inriktning av metoderna för underrättelseinhämtning som avses i 1 mom. i sådana fall då en part i kommunikationen som åtnjuter immunitet mot underrättelseinhämtning deltar i verksamhet som är föremål för civil underrättelseinhämtning och som utgör ett allvarligt hot mot den nationella säkerheten. Tillämpningen av undantaget ska vara oberoende av vilken typ av verksamhet enligt 3 mom. som den civila underrättelseinhämtningen riktar sig mot. Användningen av metoder för underrättelseinhämtning som inte berörs av förbudet mot avlyssning och observation förutsätter med andra ord inte en sådan direkt koppling till samma slags verksamhet som föreskrivs i 10 kap. 52 § 4 mom. i tvångsmedelslagen beträffande brott.

42 §. *Granskning av upptagningar och handlingar från civil underrättelseinhämtning.* Enligt paragrafen ska en polisman som hör till befälet vid skyddspolisen eller en av denne förordnad tjänsteman utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av en metod för civil underrättelseinhämtning.

Förslagen till reglering av metoderna för underrättelseinhämtning och skyddet av dem utgår från att en polisman som hör till befälet vid skyddspolisen har en central ställning när han eller hon vidtar dessa åtgärder och är skyldig att övervaka att de utförs lagenligt. Således föreslås det att polismannen också ska svara för granskningen av upptagningar och handlingar som uppkommit vid användningen.

Om en polisman som hör till befälet vid skyddspolisen förordnar en annan tjänsteman att granska upptagningar och handlingar, ska den som gett förordnandet svara för att tjänstemannen i fråga har nödvändiga kunskaper och färdigheter samt erfarenheter så att personen klarar av uppgiften.

Granskningsskyldigheten ska gälla alla metoder för underrättelseinhämtning. Granskningen har stor betydelse med tanke på att den polisman som hör till befälet vid skyddspolisen som ansvarar för verksamheten verkligen ska kunna övervaka att metoderna används lagenligt. Bland annat material som omfattas av förbud mot underrättelseinhämtning och annat material som myndigheten för militär underrättelseinhämtning inte får inhämta med hjälp av metoder för underrättelseinhämtning ska strykas ur upptagningarna och handlingarna. Det är nödvändigt att granskningen görs utan dröjsmål bland annat för att man ska kunna fastställa och utplåna det material som omfattas av förbud mot underrättelseinhämtning.

Vid granskning av upptagningarna kan man dra nytta av tekniska anordningar, metoder eller program så att granskningen omfattar bara sådana avsnitt i upptagningarna som innehåller information. På detta sätt kan man stryka eller förbigå de tomma avsnitten.

Paragrafen överensstämmer i sak med bestämmelserna i 5 kap. 51 §.

43 §. *Undersökning av upptagningar från civil underrättelseinhämtning.* Enligt paragrafen får upptagningar som uppkommit vid användningen av metoder för civil underrättelseinhämtning undersökas endast av domstol och en polisman som hör till befälet vid skyddspolisen. Enligt förordnande av polismannen som hör till befälet vid skyddspolisen eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en expert eller av någon annan som anlitas för inhämtande av information.

Paragrafen överensstämmer med bestämmelsen i 5 kap. 52 §. Om en polisman som hör till befälet vid skyddspolisen förordnar en annan tjänsteman att granska upptagningar och handlingar, ska den som gett förordnandet svara för att tjänstemannen i fråga har nödvändiga kunskaper och färdigheter samt erfarenheter så att personen klarar av uppgiften. I praktiken ska en polisman som hör till det befäl som svarar för granskningen samt annan tjänsteman ha fått utbildning i användningen av metoder för underrättelseinhämtning.

44 §. *Utlämnande av information som erhållits vid civil underrättelseinhämtning för brottsbekämpning.* I paragrafen föreskrivs om så kallade brandmurar. Information som inhämtats med stöd av befogenheter som gäller underrättelseverksamhet får i princip inte användas för andra syften än för att skydda den nationella säkerheten. I bestämmelsen om brandmur ingår vissa undantag från ändamålsbegränsningen.

Paragrafen täcker i viss mån också ärenden som hör till tjänstgöringsskyldigheten för en polisman vid skyddspolisen. I detta avseende hänvisas till det som anges under 36 §.

Enligt första meningen i 1 mom. ska skyddspolisen utan obefogat dröjsmål underrätta centralkriminalpolisen om det medan en metod för underrättelseinhämtning används framkommer att det finns skäl att misstänka ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst sex år. I praktiken ska anmälan göras så snart det är möjligt. Om det finns en mycket viktig och befogad orsak till att fördröja anmälan, gör bestämmelsen det möjligt att fördröja anmälan med högst några dagar. Bestämmelsen ålägger inte skyddspolisen en aktiv skyldighet att från de uppgifter som inhämtats med hjälp av metoder för underrättelseinhämtning gallra ut sådana uppgifter som är av betydelse för utredningen av brottet och som uttrycks med ordet ”framkommer”.

Det är motiverat med låga förväntningar när det gäller uppgiftens sannolikhet, vilket uttrycks med ”det finns skäl att misstänka”. I detta sammanhang finns det skäl att misstänka ett brott, om de som noggrant prövar olika frågor på basis av tillgänglig aktuell information intuitivt upplever att ett brott har begåtts. Det behöver också finnas element av ett sådant brott för vilket det föreskrivna strängaste straffet är fängelse i minst sex månader. Det är inte fråga om tröskeln för när ett brott ska avslöjas, eftersom det enligt det som sägs ovan inte finns någon aktiv skyldighet att gallra ut brottsuppgifter, och målet således inte heller är att klarlägga om det föreligger en sådan grund som avses i 3 kap. 3 § 1 mom. i förundersökningslagen för att inleda en förundersökning.

Skyddspolisen ska ansvara för att det görs en anmälan till centralkriminalpolisen. Centralkriminalpolisen ska i sin tur se till att anmälan går vidare till den myndighet till vilken det hör att förrätta förundersökning eller besluta om att förundersökning ska förrättas. Förundersökningsmyndigheterna räknas upp i 2 kap. 1 § i förundersökningslagen (805/2011). I vissa situationer är det däremot åklagaren som fattar beslut om förundersökning. Till exempel när det är fråga om ett brott som misstänks ha begåtts utomlands, krävs det enligt 1 kap. 12 § i strafflagen (205/1997) riksåklagarens åtalsförordnande för att brottet ska prövas i Finland. I en sådan situation ska centralkriminalpolisen föra anmälan vidare till riksåklagarämbetet på samma sätt

som vid misstanke om polisbrott då särskilda undersökningsarrangemang enligt 2 kap. 4 § i förundersökningslagen ska tillämpas.

Enligt första meningen i momentet är det skyddspolisens skyldighet att anmäla så kallade särskilt grova brott, dvs. brott för vilka det föreskrivna strängaste straffet är fängelse i minst sex år. Sådana sanktionshot leder redan i sig till ett så starkt intresse för att utreda brotten och realisera straffansvaret att det med tanke på det straffrättsliga systemets trovärdighet är nödvändigt att underrätta den behöriga myndigheten om brotten, i detta fall centralkriminalpolisen.

Förutom anmälan ska skyddspolisen också lämna nödvändiga uppgifter om brottet till centralkriminalpolisen. Hur nödvändiga de uppgifter är som ska lämnas ut kan bedömas i första hand utifrån vad som ovillkorligen krävs för att inleda en förundersökning. Utlämningen av sådana uppgifter, som händelser och sakägare eller andra uppgifter som avses i 1 kap. 2 § 1 mom. i förundersökningslagen kommer naturligtvis i fråga bara i den omfattningen som skyddspolisen överhuvudtaget har fått uppgifter genom att använda metoder för underrättelseinhämtning. Hur nödvändiga uppgifterna är kan i andra hand bedömas med tanke på bevisningen, och det är då viktigt att känna till sådana omständigheter som behöver påvisas till stöd för yrkandet om straff för det misstänkta brottet.

Enligt andra meningen i momentet får genom beslut av chefen för skyddspolisen anmälan skjutas upp med högst ett år åt gången, om det är nödvändigt för att skydda den nationella säkerheten eller liv eller hälsa. På detta sätt blir tröskeln hög för att skjuta upp anmälan (”nödvändigt”). Anmälan får skjutas upp med högst ett år åt gången. Det är dock möjligt att fatta flera beslut, om det för varje gång kan anges adekvata grunder.

Det första beslutet om uppskov bör fattas omedelbart om det i samband med användningen av en metod för underrättelseinhämtning framkommit sådana brottsuppgifter som avses i bestämmelsen. Om det är motiverat med en anmälan efter att tidsfristen på ett år har gått ut, ska det nya beslutet fattas i god tid innan tidsfristen går ut. Om det uppstår en intervall mellan det att tidsfristen går ut och beslutet fattas, är följden för det första att uppgifterna ska lämnas ut till centralkriminalpolisen utan ogrundat dröjsmål. För det andra kan den som varit föremål för informationsinhämtningen under den mellanliggande tiden från tidsfristens utgång till beslutet med åberopande av partsoffentlighet få vetskap om användningen av en metod för underrättelseinhämtning.

Uppskov är möjligt först och främst om det är nödvändigt för att trygga den nationella säkerheten. Tröskeln för ”nödvändigt” ska vara hög och med det avses att det är en sistahandsåtgärd, dvs. att den nationella säkerheten i enskilda fall inte kan tryggas på något annat sätt än genom att skjuta upp anmälan. Genom motiveringen i fråga kan man säkerställa att informationsinhämtningen når en punkt då en anmälan inte leder exempelvis till att uppgifterna om skyddspolisens taktiska eller tekniska metoder röjs i sådana fall då ett avslöjande skulle innebära ett hot mot den nationella säkerheten. Motiveringen för att skjuta upp anmälan kan också ha att göra med exempelvis behovet av att undvika den förundersökning som ofrånkomligen inleds om det görs en anmälan och den skada som detta orsakar för Finlands bilaterala relationer liksom för landets förutsättningar att ingå i det internationella samarbetet. Tryggandet av den nationella säkerheten ska när en anmälan skjuts upp i princip tolkas på samma sätt som tryggandet av statens säkerhet har tolkats enligt 5 kap. 58 § 2 mom. i polislagen som handlar om underrättelse om hemligt inhämtande av information.

För det andra är uppskov möjligt om det är nödvändigt för att skydda liv eller hälsa. Exempelvis till följd av åtgärder som vidtagits för att skydda en person kan denna grund falla bort efter en viss tid, och efter det kan den som varit föremål för informationsinhämtningen underrättas.

Med stöd av motiveringen i fråga kan man exempelvis säkerställa att informationsinhämtningen når en punkt då en anmälan inte längre medför någon risk för säkerheten i arbetet.

I 4 mom. föreskrivs om övriga kriterier som ligger till grund för bedömningen av ett uppskov av anmälan. Med beaktande av att skyddspolisens beslut om uppskov innebär ett undantag från den anmälningsskyldighet som är utgångspunkten, bör det vara motiverat att genast informera också underrättelseombudsmannen om detta. Denna bestämmelse finns i 61 §. Efter att ha fått informationen kan underrättelseombudsmannen göra en egen bedömning bland annat av huruvida det mot bakgrund av kriterierna i detta moment och 4 mom. är möjligt att betrakta beslutet om uppskov som försvarbart samt vid behov utnyttja sin granskningsrätt för att övervaka lagligheten i besluten om uppskov.

Enligt tredje meningen i momentet får skyddspolisen anmäla ett brott till centralkriminalpolisen om det för brottet föreskrivna strängaste straffet är fängelse i minst tre år. I momentet fastställs således ett förbud mot utlämning av uppgifter som stöder sig på ett hot om sanktioner på minst tre år för utredning av brottet. Uppgifter om brott för vilka det föreskrivna strängaste straffet underskrider tre år ska alltid lämnas utan anmälan till centralkriminalpolisen för utredning. Med beaktande av dels den anmälningsskyldighet som föreslås i andra meningen i 1 mom., dels det förbud mot anmälan som följer av denna mening, får skyddspolisen när det gäller brott för vilka hotet om sanktioner är minst tre år och högst sex år och redan utförda brott tid för att överväga om den ska anmäla ett sådant brott till centralkriminalpolisen eller inte. Prövningen är dock bunden till de kriterier som anges i 3 mom. Beträffande de nödvändiga brottsuppgifter som ska lämnas ut i samband med anmälan hänvisas till det som anges ovan.

Enligt första meningen i 2 mom. ska skyddspolisen utan dröjsmål underrätta den behöriga myndigheten, om det medan en metod för underrättelseinhämtning används framkommer ett brott för vilket det föreskrivna strängaste straffet är minst sex år och som ännu kan förhindras. Med behörig myndighet avses utöver förundersökningsmyndigheter exempelvis nödcentraler. I motsats till vad som vanligen är fallet är skyldigheten att anmäla det brott som avses i bestämmelsen bundet till att anmälan ska göras ”utan dröjsmål”. När det gäller responsen medför meningen i fråga en betydligt strängare skyldighet för skyddspolisen att anmäla det brott som avses i bestämmelsen. I praktiken ska anmälan göras så snabbt som mänskligt agerande och sättet för anmälan gör det möjligt.

Enligt andra meningen i momentet får skyddspolisen till den behöriga myndigheten överlämna information som fåtts genom användning av en metod för underrättelseinhämtning för förhindrande av ett sådant brott som ännu kan förhindras och för vilket det föreskrivna strängaste straffet är fängelse i minst två år. För gärningar för vilka hotet om straff underskrider detta gäller däremot förbud mot utlämning av uppgifter. Information som ska lämnas ut till den behöriga myndigheten kan ha att göra med förhindrande av brottet, men också med avslöjande av det eller exempelvis med att fastställa tröskeln för när en förundersökning ska inledas. Bestämmelser om de kriterier som styr prövningen av informationsutlämningen finns i 3 mom. Vad gäller brottsuppgifter som är nödvändiga och som ska lämnas ut i samband med anmälan hänvisas till det som anges ovan i samband med 1 mom. I detta sammanhang bör man särskilt beakta brott som hotar liv och hälsa. Dessutom kan den hotpotential som vissa brott utgör för liv och hälsa tala för en anmälan. Till exempel hot om våld som är kopplat till ett evenemang för allmänheten eller en allmän plats är ett vägande skäl för anmälan. Det kan vara fråga om en situation då det utifrån observationer av en persons beteende skäligen kan antas att det finns risk för ett obehörigt angrepp som riktar sig mot andra människor som finns på platsen.

Det är klart att skyddspolisen trots den anmälan som avses i 1 och 2 mom. får fortsätta pågående informationsinhämtning med stöd av detta kapitel, om förutsättningarna för använd-

ning av metoden för informationsinhämtning fortfarande finns. Bestämmelser om fortsatt informationsinhämtning för att förhindra brott som anges i 5 kap. 3 § eller högförräderi, grovt högförräderi eller olaglig militär verksamhet, dvs. brott som hör till skyddspolisens bekämpningsansvar, finns i 5 §.

När man överväger att skjuta upp en anmälan enligt 1 mom. eller göra en anmälan enligt 1 eller 2 mom. om ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst tre år, eller för att förhindra ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år, ska enligt 3 mom. i paragrafen vid prövningen beaktas vilket betydelse det har att brottet utreds eller förhindras för det allmänna och det enskilda intresset. I momentet sammanställs de kriterier som ska tillämpas vid bedömningen av huruvida en anmälan ska skjutas upp och en prövningsbaserad anmälan göras om ett brott som redan har begåtts eller ännu kan förhindras. Skyddspolisens prövning av dessa åtgärder är således inte fri, utan bunden även till bedömningskriterierna i 3 mom. Med tanke på syftet med användningen av metoderna för underrättelseinhämtning är det obestridligen så att det främsta bedömningskriteriet i fall som gäller prövningsbaserad utlämning av brottsuppgifter hur utlämningen påverkar den nationella säkerheten. Vid uppskov av en anmälan ska skyddspolisen dock ställa den nationella säkerheten eller skyddet av liv och hälsa i relation till intresset för att brottet utreds.

Enligt 1 mom. i paragrafen får chefen för skyddspolisen skjuta upp en anmälan med högst ett år åt gången. För att chefen för skyddspolisen verkligen ska kunna bedöma betydelsen av att brott utreds eller förhindras för det allmänna och det enskilda intresset, kan denne i enskilda fall kräva att centralkriminalpolisen eller lokalpolisen underrättas innan beslutet fattas. På detta sätt kan man i fråga om intressena ovan säkerställa att chefen för skyddspolisen genom sin prövning kan tillgodose dem så fullständigt som möjligt.

När det är fråga om att göra en prövningsbaserad anmälan av ett brott som redan har begåtts eller som ännu kan förhindras, gäller det vid bedömningen att inrikta sig på frågan om hur en anmälan kommer att påverka möjligheterna att utreda eller förhindra brottet med tanke på ett allmänt eller enskilt intresse. Utgångspunkt för bedömningen är det allmänna och det enskilda intresset. Beträffande det allmänna intresset är vikten av att brottet förhindras eller utreds större ju allvarligare brottsmisstanke det är fråga om. Med tanke på det allmänna intresset bör man när det är fråga om ett brott som redan har begåtts också beakta om uppskov eller prövningsbaserad anmälan överhuvudtaget är möjligt om det inte är i högsta grad sannolikt att brottet förblir ouppklarat. Utredningen av brottet sätts inte på spel åtminstone inte om informationen i sig utgör ett väsentligt bevis på att gärningsmannen är skyldig till brottet. Å andra sidan är det också viktigt att bedöma om en anmälan eventuellt kan skada det allmänna intresset och om nackdelarna med en anmälan är större än den nytta som uppnås med den. Med tanke på det enskilda intresset är det åter av betydelse till exempel om en anmälan bedöms göra det möjligt att återställa en målsägandes egendom som förvärvats genom brottet eller om den förverkandepåföljd som utdömts på grund av brottet eller skadeståndet till målsägande verkställs. Å andra sidan inbegriper enskilt intresse också en bedömning av om en anmälan kan medföra fara för någons liv eller hälsa, vilket i princip talar mot en anmälan.

Enligt 4 mom. i paragrafen får information som fåtts genom användning av en metod för underrättelseinhämtning alltid överlämnas som en utredning som stöder det att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada. Med hänsyn till objektivitetsprincipen vid förundersökningar samt vars och ens rätt till en rättvis rättegång och personlig frihet är det klart att man vid en förundersökning ska förhålla sig desto mer allvarligt till en begäran om en utredning som stöder det att någon är oskyldig ju större faran är att personen anhålls, straffas, blir föremål för något annat tvångsmedel, åtalas eller döms till straff eller andra straffrättsliga påföljder på felaktiga grunder. Samma omständigheter ska beaktas på tjänstens vägnar också då

skyddspolisen överväger att på eget initiativ överlämna information som stöder en oskyldig. Detta kan komma i fråga närmast i fall som avses i 5 mom., dvs. när förundersökningsmyndigheten har meddelat skyddspolisen att den kommer att inleda en förundersökning, använda en förundersökningsåtgärd eller vidta en åtgärd som syftar till att förhindra ett brott beträffande en person som varit eller fortfarande är föremål för skyddspolisens informationsinhämtning. En begäran från den misstänkte kan i praktiken komma i fråga bara om personen har underrättats om användningen av en metod för underrättelseinhämtning.

Den fara eller skada som avses i momentet behöver inte nödvändigtvis vara kopplad till ett brott, utan det kan vara fråga om exempelvis att förhindra en olycka. Ju större faran är för någons liv, hälsa eller frihet, desto högre är tröskeln för att låta bli att lämna en anmälan till exempel till en behörig myndighet. Anmälan kan göras också till en privatperson eller en organisation, om det är nödvändigt för att förhindra en betydande miljö-, egendoms- eller förmögenhetsskada.

Om en förundersökningsmyndighet inleder en förundersökning eller vidtar en förundersökningsåtgärd eller om en behörig myndighet inleder en åtgärd som syftar till att förhindra ett brott utifrån en anmälan som avses i denna paragraf, ska förundersökningsmyndigheten eller den behöriga myndigheten enligt 5 mom. innan förundersökningen inleds, förundersökningsåtgärden vidtas eller den brottsbekämpande åtgärden vidtas anmäla detta till skyddspolisen. Syftet med momentet är att hålla skyddspolisens informerad om lägesbilden om vilka åtgärder förundersökningsmyndigheterna eller de övriga behöriga myndigheterna vidtagit utifrån de uppgifter som skyddspolisen lämnat till dem samt säkerställa att det görs en anmälan om användningen av en metod för underrättelseinhämtning i situationer som avses i 46 § 5 mom. Enligt den sistnämnda bestämmelsen behöver den som varit föremål för inhämtning av information inte underrättas om systematisk observation, förtäckt inhämtande av information, en täckoperation, bevisprovokation genom köp, styrd användning av informationskällor och platsspecifik underrättelseinhämtning, om inte förundersökning har inletts i ärendet. Bestämmelser om när förundersökning sak göras finns 3 kap. 3 § i förundersökningslagen (805/2011). Med förundersökningsåtgärder avses bland annat förhör och konfrontation. Till de åtgärder som vidtas för att förhindra brott hör bland annat gripande av en person, tillträde till utrymmen som omfattas av hemfrid och offentlig frid eller avspärrning av platser och områden.

45 §. *Utplåning av information som erhållits vid en metod för underrättelseinhämtning.* Enligt 1 mom. ska information som fåtts genom en metod för underrättelseinhämtning utplånas utan dröjsmål efter att det framgått att den inte behövs för att skydda den nationella säkerheten.

Momentet ska gälla all information som inhämtats med hjälp av en metod för underrättelseinhämtning. Innehållet i den information som redan inhämtats med hjälp av metoden för underrättelseinhämtning bör mycket snabbt framgå för att man ska få svar på frågan om den behövs för att skydda den nationella säkerheten eller om den kan utplånas.

Enligt 2 mom. får informationen dock bevaras och lagras i ett register som avses i lagen om behandling av personuppgifter i polisens verksamhet, om detta behövs i sådana fall som avses i 44 §.

Uppgifter som inhämtats med hjälp av en metod för underrättelseinhämtning och som inte är knutna till skyddet av den nationella säkerheten ska i princip utplånas. Det finns då risk för att man samtidigt utplånar material som avses i 44 §. Det är därför nödvändigt att tillåta avvikelser från skyldigheten att utplåna material för att man vid behov ska ha tillgång till material som är nödvändigt för att utreda och förhindra till exempel grova brott eller som stöder det att någon är oskyldig.

Enligt 3 mom. i paragrafen ska sådana basstationsuppgifter som avses i 7 § utplånas efter att det har framgått att de inte behövs för att skydda den nationella säkerheten. Bestämmelsen överensstämmer med 5 kap. 55 § 3 mom. med den skillnaden att behovet av uppgifter i detta moment är knutet till skyddet av den nationella säkerheten.

Bestämmelser om utplåning av uppgifter finns också i lagen om behandling av personuppgifter i polisens verksamhet (761/2003).

46 §. *Utplåning av information som erhållits i en brådskande situation.* Om en polisman som hör till befälet vid skyddspolisen i en brådskande situation enligt 7 § 1 mom., 8 § 1 mom., 11 § 1 mom., 12 § 1 mom., 13 § 1 mom., 14 § 1 mom. eller 27 § 2 mom. har beslutat att teleövervakning, inhämtande av basstationsuppgifter, teknisk avlyssning, optisk observation, teknisk spårning av en person, teknisk observation av utrustning eller platsspecifik underrättelseinhämtning ska inledas men domstolen anser att det inte finns förutsättningar för åtgärden, ska enligt paragrafen användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Informationen får dock användas under samma förutsättningar som en uppgift får användas i de fall som avses i 44 § 1 eller 2 mom., om det kan antas att ett brott har begåtts, för vilket det strängaste föreskrivna straffet är fängelse i minst sex år eller om det framgår att ett brott är på gång, för vilket det strängaste föreskrivna straffet är fängelse i minst sex år, och brottet ännu kan förhindras.

Efter det brådskande beslutet ska underrättelseombudsmannen informeras om domstolens negativa beslut för prövning av om förfarandet med brådskande beslut är lagenligt. När det gäller information som fåtts med stöd av ett brådskande beslut är det i princip fråga om lagligt inhämtad information. Om domstolen efteråt anser att det inte har funnits någon grund för det brådskande beslutet kan detta, beroende på hur allvarligt det eventuella förfarandefelet är, leda till att den information som inhämtats med metoden för underrättelseinhämtning inte kan användas som en utredning till stöd för att någon är skyldig eller som bevis för att någon är skyldig. Domstolen kan i sitt negativa beslut också uppge hur värdefulla de uppgifter är för utredningen av brottet som den fått med stöd av sitt brådskande beslut med beaktande av hur allvarlig rättskränkningen är i samband med sättet att skaffa uppgifterna. Som en allmän utgångspunkt vid prövningen kan man se dels intresset av att lösa frågan (brottets allvar) som en aspekt som talar för användningen av uppgifterna, dels de skadliga följderna av användningen som en omständighet som talar för ett förbud mot användning. Användningen kan å ena sidan kränka den misstänktes rättssäkerhet, å andra sidan vara en hjälp att finna den materiella sanningen samt medverka till att tillgodose målsägandes rättigheter. Som en allmän utgångspunkt kan man också se det faktum att den information som fåtts med stöd av ett brådskande beslut kan användas som stöd för att den åtalade är oskyldig.

I 2 mom. föreskrivs om utplåning av den information som i en brådskande situation fåtts genom kopiering. Det gäller en motsvarande situation som i 1 mom. Om en polisman vid skyddspolisen i en brådskande situation har beslutat om kopiering, men en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning anser att det inte finns förutsättningar för åtgärden, ska användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Information som fåtts på detta sätt får dock användas under samma förutsättningar som en uppgift får användas i de fall som avses i 44 § 1 eller 2 mom., om det kan antas att ett brott har begåtts, för vilket det strängaste föreskrivna straffet är fängelse i minst sex år eller om det framgår att ett brott är på gång, för vilket det strängaste föreskrivna straffet är fängelse i minst sex år, och brottet ännu kan förhindras.

47 §. *Underrättelse om användning av metod för underrättelseinhämtning.* Enligt första meningen i 1 mom. ska den som vid civil underrättelseinhämtning har varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning och teknisk observation samt kopiering som riktar sig mot ett meddelande eller sådan kopiering av en försändelse som riktar sig mot ett meddelande utan dröjsmål underrättas om detta skriftligen efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts. Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om underrättelsen.

I momentet anges de metoder för underrättelseinhämtning om vilka den som varit föremål för informationsinhämtningen ska underrättas. Det är fråga om metoder som innebär ingrepp i skyddet av ett förtroligt meddelande som tillhör en person som är föremål för informationsinhämtning. I bestämmelsen kopplas skyldigheten att underrätta den som är föremål för underrättelseinhämtning om användningen av metoder för underrättelseinhämtning till tidpunkten för när informationsinhämtningen har avslutats. Informationsinhämtningen kan ha avslutats antingen på grund av att dess syfte att avslöja en verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten har uppnåtts eller för att informationsinhämtningen har visat sig resultatlös.

Underrättelsen ska vara specificerad på ett sådant sätt att objektet vid behov kan försöka reda ut grunderna för användningen av metoden för underrättelseinhämtning. I underrättelsen ska anges till exempel vilken metod det är fråga om samt var och när metoden har använts. Myndigheten behöver inte avslöja detaljerna kring det taktiska och tekniska genomförandet. Objektet kan underrättas exempelvis per brev till den adress som senast har meddelats myndigheten. Ingen annan än den som varit föremål för underrättelseinhämtning behöver underrättas om att en metod för underrättelseinhämtning har använts, även om någon annan person i praktiken blivit föremål för åtgärden. Bara de personer som i själva verket varit föremål för informationsinhämtning ska således omfattas av underrättelseskyldigheten, dvs. de personer för vilkas del ett yrkande har framställts eller ett beslut fattats om användning av en metod för underrättelseinhämtning.

När användningen av en metod för underrättelseinhämtning de facto har avslutats innan tillståndets eller beslutets giltighetstid gått ut, och inget nytt tillstånd har sökts eller beslut fattats om att fortsätta underrättelseinhämtningen, ska objektet underrättas om den faktiska tidpunkten då informationsinhämtningen avslutades. Om informationsinhämtningen fortsätter med stöd av ett fortsatt tillstånd eller beslut, ska objektet underrättas antingen om tidpunkten för när åtgärden verkligen avslutas eller när giltighetstiden för tillståndet eller beslutet går ut. Med tanke på informationsinhämtningens kontinuitet kan några dagars avbrott mellan besluten godtas.

Enligt andra meningen i 1 mom. ska den som varit föremål för inhämtning av information dock underrättas om användningen av metoden för underrättelseinhämtning senast ett år efter att användningen av den har upphört. Om användningen av en metod verkligen har avslutats innan tillståndets eller beslutets giltighetstid gått ut, och inget nytt tillstånd har sökts, ska tidsfristen på ett år räknas från den verkliga tidpunkten för avslutandet. Om informationsinhämtningen har upphört när giltighetstiden för tillståndet eller beslutet gick ut, ska tidsfristen på ett år räknas från denna tidpunkt. I fråga om retroaktiv informationshämtning ska tidsfristen räknas från den tidpunkt då tillståndet beviljades eller beslutet fattades, trots att information ännu inte har fåtts.

Om det i fråga om samma person som är föremål för informationsinhämtning har fattats ett nytt beslut om användning av samma metod för informationsinhämtning ska tidsfristen på ett år räknas från den tidpunkt då den sista informationsinhämtningen i ärendet faktiskt avslutades

eller från utgången av tillståndets eller beslutets giltighetstid. Med tanke på informationsinhämtningens kontinuitet kan några dagars avbrott mellan beslutens giltighet godtas.

Enligt 2 mom. i paragrafen får på yrkande av en polisman som hör till befälet vid skyddspolisen domstolen besluta att underrättelsen enligt 1 mom. till den som varit föremål för åtgärden får skjutas upp med högst två år åt gången, om det är motiverat för att trygga pågående användning av metoden för underrättelseinhämtning, garantera den nationella säkerheten eller skydda liv eller hälsa. Domstolen får besluta att underrättelsen ska utebli, om det är nödvändigt för att garantera den nationella säkerheten eller skydda liv eller hälsa.

Domstolen beslutar att en underrättelse skjuts upp eller uteblir, även om en polisman som hör till befälet vid skyddspolisen har fattat beslut om metoden för underrättelseinhämtning. Enligt förslaget kan underrättelsen skjutas upp med högst två år åt gången. Nya uppskov ska beviljas bara undantagsvis. I stället för upprepade uppskov av en underrättelse är det att föredra att man ansöker om att helt få låta bli att underrätta objektet, förutsatt att det finns förutsättningar för det, eftersom en underrättelse som görs efter exempelvis tio år inte har någon betydelse för objektet. Ansökan om uppskov och nya uppskov ska sökas innan den utsatta tiden går ut.

En grund för ett eventuellt uppskov är först och främst att trygga användningen av en pågående metod för underrättelseinhämtning. Informationsinhämtningen kan gälla vilken aktuell underrättelseoperation som helst, också en militär underrättelseoperation. Ett uppskov ska vara möjligt också för att trygga den nationella säkerheten. Begreppet tryggande av den nationella säkerheten behandlas i motiveringen till 44 §. Dessutom ska det vara möjligt att skjuta upp en underrättelse för att skydda liv eller hälsa. Förutsättningen för uppskov är att det är motiverat. Tröskeln för uppskov är således inte särskilt hög.

Man kan underlåta att underrätta objektet bara om det är nödvändigt för att trygga den nationella säkerheten eller för att skydda liv eller hälsa. Tröskeln för att helt låta bli att underrätta objektet ska å sin sida vara hög, vilket beskrivs med uttrycket ”nödvändigt”.

Om domstolen inte beviljar uppskov eller inte godkänner att man underlåter att underrätta objektet, får den som framställt yrkandet klaga över beslutet hos Helsingfors hovrätt på det sätt som anges i 35 §.

Om den som är föremål för inhämtande av information inte är identifierad vid utgången av den föreskrivna tid eller det uppskov som avses i 1 eller 2 mom., ska enligt 3 mom. han eller hon utan ogrundat dröjsmål skriftligen underrättas om underrättelseinhämtningen när identiteten har utretts. Den som är föremål för informationsinhämtning men inte har identifierats kan naturligtvis inte underrättas. Om identiteten hos den som är föremål för informationsinhämtning senare klarläggs ska det dock lämnas en underrättelse. Sådana situationer kan också bilda ett undantag från de tidsfrister som föreskrivs i paragrafen, eftersom dessa i vissa fall inte kan iakttas. Om en identifierad person som är föremål för informationsinhämtning är försvunnen, kommer det inte att krävas några omfattande åtgärder av skyddspolisen bara för underrättelsen. För en underrättelse ska det vara tillräckligt att det görs en efterlysning i ärendet (till exempel anmälan om vistelseort).

Enligt 4 mom. i paragrafen ska den domstol som beviljat tillståndet samtidigt skriftligen informeras om underrättelsen. Då användningen av en metod för underrättelseinhämtning grundar sig på ett domstolsbeslut, ska också domstolen samtidigt informeras om underrättelsen. Således ska också Helsingfors tingsrätt delges information om att objektet underrättats om användningen av en metod för underrättelseinhämtning som förutsätter tillstånd.

Om skyddspolisen fortsätter inhämtandet av information med stöd av 5 §, ska enligt 5 mom. bestämmelserna om underrättelse om hemligt inhämtande av information i 5 kap. 58 § iakttas. I en situation då informationsinhämtning som inletts genom användning av en metod för underrättelseinhämtning fortsätter genom användning av en metod för hemligt inhämtande av information ska föremålet för informationsinhämtningen samt domstolen underrättas om detta liksom om beslut om att underrättelsen skjuts upp eller helt och hållet uteblir enligt 5 kap. 58 § i polislagen. I de situationer som avses i momentet ska underrättelse lämnas om användningen av såväl en metod enligt 5 kap. i polislagen som en metod för underrättelseinhämtning. Underrättelsen om användningen av en metod för underrättelseinhämtning ska i detta sammanhang prövas enligt den sistnämnda paragrafen.

Enligt 6 mom. behöver den som vid civil underrättelseinhämtning varit föremål för inhämtande av information inte underrättas om systematisk observation, förtäckt inhämtande av information, en täckoperation, bevisprovokation genom köp, styrd användning av informationskällor, platsspecifik underrättelseinhämtning, kopiering som riktas mot annat än ett meddelande och kopiering av en försändelse som riktas mot annat än ett meddelande, om inte förundersökning har inletts i ärendet utifrån en anmälan enligt 44 §. Underrättelse om platsspecifik underrättelseinhämtning lämnas till den som har varit föremål för användningen av metoden för underrättelseinhämtning och vid behov också till platsens ägare eller innehavare. Beträffande den kopiering som avses i bestämmelsen och kopiering av försändelser ska den som varit föremål för informationsinhämtningen underrättas. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen iakttas. När det gäller användningen av de metoder för underrättelseinhämtning som anges i momentet behöver däremot ingen underrättelse lämnas, om det i det ärende som är föremål för underrättelseinhämtningen inte inleds någon förundersökning utifrån en anmälan enligt 44 §.

I 7 mom. i paragrafen föreskrivs om underrättelser som ska lämnas till statliga aktörer. Enligt bestämmelsen behöver den som varit föremål för inhämtande av information inte underrättas om användningen av en metod för underrättelseinhämtning, om föremålet har varit en statlig aktör eller en aktör som är jämställbar med en sådan. Kommunikationen i en främmande stats myndighetsorganisation åtnjuter inte skydd för förtroliga meddelanden och en underrättelse kommer mycket sällan i fråga, om föremål för informationsinhämtningen har varit en myndighet i den främmande staten, dvs. en statlig aktör. Till bestämmelsens tillämpningsområde hör också indirekta aktörer för den statliga aktören.

Inom underrättelseinhämtning som avser utländska förhållanden finns det ingen skyldighet att underrätta objektet om användningen av en metod för underrättelseinhämtning (39 § 3 mom.). Dessutom är det nödvändigt att beakta också de situationer då en metod för underrättelseinhämtning används på en statlig aktör på Finlands territorium. Såväl inom underrättelseinhämtning som avser utländska förhållande som vid användning av en metod för underrättelseinhämtning som gäller en statlig aktör på finskt territorium är verksamheten så gott som utan undantag förenad med utrikespolitiska och eventuellt andra känsliga omständigheter, varvid det inte är motiverat att underrätta objektet. Bestämmelsen förhindrar dock inte en underrättelse, vilket uttrycks genom ”finns det ingen skyldighet att underrätta”.

Enligt 8 mom. i paragrafen ska i fråga om handläggning av underrättelseärenden i domstol 35 § iakttas. Med hänvisningen avses i praktiken att också underrättelseärenden handläggs vid Helsingfors tingsrätt. Liksom i samband med tillståndsärenden som avser metoder för underrättelseinhämtning ska också vid behandlingen av underrättelseärenden särskild vikt fästas vid att skyddet av uppgifter i handlingar och datasystem tryggas genom nödvändiga förfaranden och datasäkerhetsarrangemang.

48 §. *Protokoll.* Efter det att användningen av en metod för underrättelseinhämtning upphört ska det enligt paragrafen utan ogrundat dröjsmål upprättas ett protokoll över användningen av metoden. För att möjliggöra rättslig övervakning av verksamheten är det nödvändigt att användningen av metoderna för underrättelseinhämtning dokumenteras. Genom förordning av statsrådet får det enligt 62 § 1 mom. utfärdas närmare bestämmelser om dokumenteringen av åtgärderna för övervakningen.

Protokollföringen av de hemliga metoder för informationsinhämtning som enligt 5 kap. i polislagen används för närvarande regleras i statsrådet förordning om förundersökning, tvångsmedel och hemligt inhämtande av information (122/2014). Enligt 3 kap. 1 § 1 mom. i förordningen ska den som föreslagit eller beslutat om användningen av hemliga tvångsmedel enligt 10 kap. 1 § i tvångsmedelslagen eller om hemligt inhämtande av information enligt 5 kap. 1 § i polislagen (872/2011) eller en förundersökningstjänsteman som han eller hon förordnat utan ogrundat dröjsmål, dock senast inom 90 dagar efter att användningen eller inhämtandet har avslutats, upprätta ett protokoll. Enligt 2 mom. ska den tekniska observation som avses i 5 kap. 17 § 5 mom., 19 § 5 mom. och 21 § 4 mom. i polislagen protokollföras.

Det är motiverat att införa motsvarande bestämmelser som i statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information om protokollföringen av de åtgärder som ska skrivas in i ett protokoll också efter att användningen av metoderna för underrättelseinhämtning har upphört.

49 §. *Begränsning av partsoffentlighet i vissa fall.* Enligt 1 mom. i paragrafen har en person vars rättigheter eller skyldigheter saken gäller inte, trots 11 § i lagen om offentlighet i myndigheternas verksamhet (621/1999), rätt att få vetskap om användningen av en metod för underrättelseinhämtning enligt detta kapitel förrän en underrättelse enligt 47 § har gjorts. I den senast nämnda 47 § föreskrivs om underrättelse om användning av metoder för underrättelseinhämtning. Det är viktigt att partsoffentligheten begränsas innan det lämnas en underrättelse om användningen av en metod för underrättelseinhämtning på grund av att det i samband med användningen av en metod framställs handlingar som gäller statens säkerhet, dvs. omständigheter som, om det informeras om dem, strider mot ett mycket viktigt allmänt intresse.

I en kommande lag om övervakning av underrättelseverksamheten införs bestämmelser om möjligheten att anföra klagomål till underrättelseombudsmannen (11 §). Klagomål kan anföras av var och en som varit föremål för underrättelseverksamhet och anser att man inom underrättelseverksamheten kränkt hans eller hennes rättigheter eller i övrigt gått lagstridigt tillväga. En person som varit föremål för underrättelseverksamhet eller som misstänker att han eller hon varit föremål för underrättelseinhämtning kan begära att underrättelseombudsmannen prövar lagligheten i användningen av den metod för underrättelseinhämtning som personen varit föremål för (12 §).

Enligt 2 mom. i paragrafen finns bestämmelser om rätten till insyn för registrerade i lagen om behandling av personuppgifter i polisens verksamhet. Det är fråga om en informativ hänvisning till den lag som avses i bestämmelsen och enligt 45 § 1 mom. 2 punkten i lagen gäller rätten till insyn inte uppgifterna i skyddspolisens funktionella informationssystem. I 2 mom. i paragrafen föreskrivs om dataombudsmannens rätt till insyn enligt vilken dataombudsmannen på begäran av den registrerade kan kontrollera att de uppgifter om den registrerade som ingår i skyddspolisens informationssystem är lagenliga.

50 §. *Rätt att få information av privata sammanslutningar.* Trots att en sammanslutnings medlemmar, revisorer, verkställande direktör, styrelsemedlemmar eller arbetstagare är bundna av företags-, bank- eller försäkringshemlighet har skyddspolisen enligt paragrafen på begäran av en polisman som hör till befälet vid skyddspolisen rätt att få uppgifter som i enskilda fall kan

antas vara behövliga vid utredningen av sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten och som kan anses vara av betydelse för att 1) identifiera eller nå en fysisk eller juridisk person som är föremål för civil underrättelseinhämtning, eller klarlägga personens kontaktuppgifter eller hur personen förflyttar sig, 2) inrikta användningen av en metod för underrättelseinhämtning på en viss person som är föremål för civil underrättelseinhämtning, eller 3) klarlägga den ekonomiska verksamhet som antas anknyta till i 3 § avsedd verksamhet för en person eller en juridisk person som är föremål för civil underrättelseinhämtning.

Paragrafen överensstämmer till sin betydelse med 4 kap. 3 § 1 mom. i polislagen. I det här sammanhanget är syftet med begäran om information dock inte att förhindra eller utreda ett brott utan begäran är bunden till föremålen för civil underrättelseinhämtning enligt 3 §, vilket framgår av formuleringen i paragrafen ”vid utredningen av sådan verksamhet som är föremål för civil underrättelseinhämtning”.

Med uttrycket som gäller utredning av verksamheten avses inte utredning (av ett brott) i den mening som avses i förundersökningslagen, utan det är fråga om utredning av en specifik verksamhet som utgör ett allvarligt hot mot den nationella säkerheten. Med utredning avses således att man sammanställer uppgifter genom att samla in information från olika källor, och den begäran om information som avses i paragrafen är ett sätt att samla in viktig information om dem som är föremål för civil underrättelseinhämtning.

Sannolikheten i paragrafen anges genom uttrycken ”kan antas vara behövliga” och ”kan anses vara av betydelse” som kan betraktas som kriterier jämförbara med så kallade resultatförväntningar. Därför ska en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och är förtrogen med användningen av metoder för underrättelseinhämtning beakta tröskeln beträffande begäran om information när hen utför uppdraget. Även om den som framställer begäran om information inte har någon skyldighet att motivera sin begäran för den som lämnar ut informationen bör framställaren basera prövningen av sin begäran om information på objektiva omständigheter och anteckna dessa så att det är möjligt att i efterhand med de medel som står laglighetsövervakningen till buds verifiera att begäran är befogad.

Syftet med bestämmelsen är att göra det möjligt för privata instanser att lämna ut information utan att göra sig skyldiga till straffbara gärningar. De som lämnar ut information som omfattas av företags-, bank- och försäkringshemlighet ska när uppgifterna lämnas ut vara övertygade om att de handlar lagligt.

Bankhemligheten regleras i 15 kap. 14 § i kreditinstitutslagen (610/2014) och försäkringshemligheten i 30 kap. 1 § i försäkringsbolagslagen (521/2008). Enligt 30 kap. 11 § i strafflagen definieras företagshemlighet som en affärs- eller yrkeshemlighet eller någon motsvarande information om näringsverksamhet som en näringsidkare håller hemlig och vars röjande är ägnat att medföra ekonomisk skada för honom eller någon annan näringsidkare som har anförtrott honom informationen. Av betydelse är det dock att bestämmelsen i fråga tillåter att informationen ovan som omfattas av tystnadsplikt får överlämnas till skyddspolisen.

Företag har en stor mängd information som är viktig för den egna näringsverksamheten och som omfattas av företagshemlighet, såsom information om produktutveckling. Enligt paragrafen har företaget ingen skyldighet att lämna ut sådan information till skyddspolisen när det gäller information som hör till kärnan i företagshemligheten och är av betydelse för den egna företagsverksamheten eller för företagets avtalspartners, utan i begäran om information är det i princip fråga om uppgifter som specificerar kunder, anställda eller instanser som står i ett annat ekonomiskt förhållande till företaget.

Huruvida begäran om information är en engångsföreteelse ska bedömas utifrån det objekt som är föremål för civil underrättelseinhämtning. På detta sätt begränsar ett enskilt fall inte antalet begäranden om information om samma verksamhet som utgör ett allvarligt hot mot den nationella säkerheten. Enskilt fall kan vid behov inbegripa flera begäranden om information om hotet i fråga, tills hotet är avvärjt.

Den information som är föremål för begäran ska enligt 1 mom. på goda grunder anses vara av betydelse för identifieringen av en fysisk eller juridisk person som är föremål för civil underrättelseinhämtning. Med detta avses att det med sannolikhet ska vara möjligt att identifiera, få tag på eller annars klarlägga personens verksamhet, exempelvis med hjälp av hotellens gästlistor eller fartygens passagerarlistor. Enligt 2 punkten i paragrafen kan grunden för begäran vara att inrikta användningen av en metod för underrättelseinhämtning på en viss person. Detta kan innebära till exempel inköp av ett engångsabonnemang och hänvisa en begäran som gäller köparen till detaljhandelsaffären. Paragrafens 3 punkt omfattar bland annat bankförfrågningar samt andra begäranden om information som riktar sig till kreditinstitut eller aktörer inom penningöverföring för att göra det möjligt att utreda en ekonomisk verksamhet som sannolikt är kopplad till en sådan verksamhet som avses i 3 § och som utövas av en fysisk eller juridisk person som är föremål för civil underrättelseverksamhet, såsom att identifiera källorna till bankgiron som en fysisk eller juridisk person har fått eller instanser som utövar beslutanderätten i en sådan juridisk person.

51 §. *Teleföretags skyldighet att biträda civil underrättelseinhämtning.* Enligt paragrafen ska på teleföretags skyldighet att biträda tillämpas vad som i 5 kap. 61 § föreskrivs om teleföretags skyldighet att biträda.

52 §. *Ersättningar till teleföretag för biträde och lämnande av uppgifter vid civil underrättelseinhämtning.* Enligt paragrafen tillämpas bestämmelserna i 5 kap. 62 § på teleföretags rätt till ersättning för direkta kostnader som orsakats av att de har biträtt myndigheter och lämnat uppgifter. Enligt 1 mom. i paragrafen har teleföretag rätt att få ersättning av statens medel för direkta kostnader som orsakats av att företaget biträtt myndigheterna och lämnat uppgifter så som det föreskrivs i 299 § i lagen om tjänster inom elektronisk kommunikation (917/2014). Beslut om betalning av ersättning fattas av den enhet vid polismyndigheten som utfört åtgärden.

Enligt 299 § 1 mom. i lagen om tjänster inom elektronisk kommunikation har teleföretag rätt att få ersättning av statens medel för direkta kostnader för investeringar i och underhåll av system, utrustning och programvara som anskaffats enbart för att biträda myndigheter. Beslut om ersättning av kostnader fattas vid behov av Kommunikationsverket.

Enligt motiveringen (RP 221/2013 rd) till paragrafen i fråga ska ett teleföretag få ersättning för underhåll av system, apparatur och program såsom kostnader för uppdatering av program och service. Däremot ersätts inte personalkostnader för användning av apparatur och program. Syftet med ändringen är att förenhetliga lagstiftningen om ersättning av kostnader. Vid beredningen av lagstiftningen om civil underrättelseinhämtning har det inte framkommit något behov av att avvika från de lagstiftningslösningar som gäller ersättning av kostnader.

I 299 § 2 mom. i lagen om tjänster nom elektronisk kommunikation föreskrivs om rätten att begära omprövning av ett beslut som fattats av polismyndigheten. Enligt 3 mom. i paragrafen ska förvaltningsdomstolen ge Kommunikationsverket tillfälle att yttra sig.

53 §. *Användning av uppgifter som lagras av teleföretag och hänför sig till civil underrättelseinhämtning.* Enligt paragrafen får utöver vad som föreskrivs om användning av lagrade uppgifter i 157 § 1 mom. i lagen om tjänster inom elektronisk kommunikation de uppgifter som

ska lagras också användas, om uppgifterna med fog kan antas vara av synnerlig vikt för att få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten.

Enligt 157 § 1 mom. i lagen om tjänster inom elektronisk kommunikation får de uppgifter som avses i 2 och 3 mom. endast användas för att utreda och åtalspröva brott som avses i 10 kap. 6 § 2 mom. i tvångsmedelslagen. I den sistnämnda bestämmelsen föreskrivs om de brott som berättigar till teleövervakning. I förteckningen ingår följande brott: 1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år, 2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år, 3) olovligt brukande som riktat sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning, 4) utnyttjande av person som är föremål för sexhandel, lockande av barn i sexuella syften eller koppleri, 5) narkotikabrott, 6) förberedelse till brott som begås i terroristiskt syfte, deltagande i utbildning för ett terroristbrott, finansiering av terroristgrupp eller resa i syfte att begå ett terroristbrott, 7) grovt tullredovisningsbrott, 8) grovt döljande av olagligt byte, 9) förberedelse till tagande av gisslan, eller 10) förberedelse till grovt rån.

Enligt den föreslagna paragrafen får motsvarande uppgifter användas också för att få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten (3 §). Det är således inte fråga om att lagra nya uppgifter utan att använda befintliga uppgifter förutom för att utreda och åtalspröva brott också för att skydda den nationella säkerheten. Mängden lagrade uppgifter kommer inte att öka.

54 §. *Samarbete med militärunderrättelsemyndigheterna.* Enligt paragrafen ska skyddspolisen samarbeta med militärunderrättelsemyndigheterna för att den civila och militära underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt och i detta syfte, trots det som föreskrivs om sekretess, ge militärunderrättelsemyndigheterna behövliga uppgifter.

Syftet med regleringen är att främja samarbetet mellan skyddspolisen och den militära underrättelsemyndigheten så att de parallella uppgifter som de nämnda myndigheterna har inom sina respektive verksamhetsområden och som hänför sig till samma mål blir utförda på ett ändamålsenligt, ekonomiskt och smidigt sätt.

Centrala samarbetsformer är gemensam underrättelse- och analysverksamhet, ömsesidigt utbyte av uppgifter, utveckling av gemensamma underrättelsesystem, skapande av en gemensam lägesbild över hot mot säkerheten och förändringar i omvärlden, gemensamma verksamhetsplaner, ömsesidig handräckning, utbildningssamarbete och utbyte av tjänstemän.

Till samarbetsformerna hör också användning av gemensamma representanter i det internationella samarbetet, gemensam personalutbildning, samordnande av underrättelseverksamheten, utveckling av informationsinhämtningen, utveckling av enhetliga blanketter och kompatibla datasystem, gemensam beredning vid anskaffning av lokaler, materiel, apparatur och utrustning samt samordnande av verksamheten och planeringen av målen för den.

Genom kravet på samarbete säkerställs det att de civila och militära underrättelsemyndigheterna är tillräckligt medvetna om varandras informationsinhämtning så att inte exempelvis kommande underrättelseoperationer äventyras eller förhindras på grund av den andra myndighetens aktiviteter. På grund av myndigheternas resurser kan det dessutom inte ses som ändamålsenligt att underrättelsemyndigheterna inte kan dela materiel och kompetens med andra underrättelsemyndigheter. Detta gäller särskilt användningen av metoder för underrättelseinhämtning från telenät och underrättelseinhämtning som avser datatrafik.

55 §. *Samarbete med andra myndigheter och sammanslutningar.* I paragrafen föreskrivs om samarbetet mellan skyddspolisen och andra än militära underrättelsemyndigheter.

Enligt paragrafen ska skyddspolisen vid behov agera i samarbete med andra myndigheter för att sköta den civila underrättelseinhämtningen på ett ändamålsenligt sätt. Således ska också andra myndigheter vid behov kunna bistå skyddspolisen vid civil underrättelseinhämtning. Detta innebär samarbete med exempelvis centralkriminalpolisen, polisinrättningar, Tullen, Gränsbevakningsväsendet, Migrationsverket eller Kommunikationsverket.

För att nå målen för den civila underrättelseinhämtningen är det av central betydelse att samarbetet mellan myndigheterna fungerar. I samarbetet ingår utveckling av datasystem, skapande av en lägesbild över hot mot säkerheten och förändringar i omvärlden, gemensamma verksamhetsplaner, ömsesidig handräckning och utbildningssamarbete.

Samarbetet kan också omfatta taktisk verksamhet mellan myndigheter. Det kan vara fråga om exempelvis åtgärder som vidtas för att förhindra att informationsinhämtningen röjs.

Enligt 2 mom. får skyddspolisen för att genomföra sitt uppdrag avseende civil underrättelseinhämtning agera i samarbete med sammanslutningar samt till andra myndigheter och sammanslutningar trots sekretessbestämmelserna lämna ut uppgifter, om utlämnandet av uppgifterna är nödvändigt för att skydda den nationella säkerheten.

Inom civil underrättelseinhämtning kan det uppstå situationer då det för att skydda den nationella säkerheten är nödvändigt att på eget initiativ eller på begäran förmedla uppgifter till en annan myndighet. Detsamma gäller för övrigt också när uppgifter lämnas ut till en annan myndighet för att den ska kunna sköta de uppgifter som hör till den. Det är fråga om något annat än utlämning av uppgifter enligt lagen om behandling av personuppgifter i polisens verksamhet, om vilket föreskrivs i lagen i fråga.

För det första ska utlämningen av uppgifter vara ett uppdrag för skyddspolisen, vilket regleras i 10 § i polisförvaltningslagen och i viss mån i 1 kap. 1 § i denna lag. Således ska skyddspolisen göra den första prövningen av utlämningen av uppgifter i anknytning till sitt arbetsfält. För det andra ska utlämningen av uppgifter vara nödvändig. Syftet med detta är att understryka att tröskeln för att röja information måste vara hög. Information får inte lämnas ut i andra fall än sådana som klart uppfyller de i momentet angivna förutsättningarna.

Samarbetet mellan skyddspolisen och sammanslutningarna kan också ha att göra med säkerheten i företagen och bedrivas för att förhindra företagsspionage.

Enligt 3 mom. finns bestämmelser om utlämning av information till brottsbekämpning i 44 §. Hänvisningen till den så kallade brandmursbestämmelsen är nödvändig eftersom skyddet av den nationella säkerheten inbegriper bara en marginell del av brotten enligt strafflagen. Således ska uppgifterna i 44 § anmälas med stöd av paragrafen i fråga.

56 §. *Samordning av hemlig informationsinhämtning.* I paragrafen föreskrivs om samordning av skyddspolisens, militärunderrättelsemyndighetens, centralkriminalpolisens och andra myndigheters hemliga informationsinhämtning. Det är fråga om en specialbestämmelse jämfört med samarbetsbestämmelserna ovan.

Myndigheternas överlappande uppgifter och i synnerhet överlappande operationer vid hemlig informationsinhämtning kan utgöra en allvarlig säkerhetsrisk i arbetet, om myndigheterna agerar ovetande om varandra i ett hemligt informationsinhämtningsuppdrag.

När det finns flera myndigheter som har rätt att använda hemlig informationsinhämtning kan detta i vissa fall ge upphov till en risk för att såväl säkerhetsmyndigheternas allmänna roller som enskilda operationer överlappar varandra. För att förhindra denna typ av situationer på förhand och avvärja eventuella arbetsolycksfall kan det från fall till fall vara nödvändigt att myndigheterna sinsemellan samordnar användningen av hemlig informationsinhämtning.

57 §. *Internationellt samarbete*. I paragrafen föreskrivs om skyddspolisens internationella samarbete. Enligt 1 mom. får skyddspolisen samarbeta och inhämta information tillsammans med utländska säkerhets- och underrättelsetjänster för att skydda den nationella säkerheten. Med samarbete avses allt samarbete mellan å ena sidan utländska säkerhets- och underrättelsetjänster, å andra sidan skyddspolisen och motsvarande verk i andra länder. Samarbetet kan bedrivas till exempel genom utbyte av information, tekniskt stöd, utbildningssamarbete, utbyte av tjänstemän, internationell kontaktpersonsverksamhet eller annan verksamhet mellan underrättelsemyndigheterna. Med gemensamma operationer avses åter gemensamma operationer för informationsinhämtning där man kan använda de metoder för underrättelseinhämtning som anges i detta kapitel. Närmare bestämmelser om gemensamma operationer finns i 2 och 3 mom. i paragrafen och om utbyte av andra uppgifter än personuppgifter i 3 mom.

I 2 mom. föreskrivs om situationer då en polisman vid skyddspolisen deltar i skyddspolisens och en utländsk underrättelse- eller säkerhetsmyndighets gemensamma operation på den främmande statens territorium.

Om den allmänna informationsinhämtningen sker i samarbete med den stat på vars territorium metoder för underrättelseinhämtning ska användas, måste de begränsningar iakttas som den staten har ställt upp för verksamheten. Polismannen vid skyddspolisen kan då när hen deltar i en gemensam operation i en annan stat med den statens samtycke använda de metoder för underrättelseinhämtning som avses i detta kapitel eller motsvarande metoder. I detta fall får metoder för underrättelseinhämtning användas bara i den omfattning och på det sätt som tillåts av staten i fråga. Bestämmelsen ska således gälla samarbete med territorialstaten i fråga. Uttrycket ”i samarbete med” kan anses täcka också gemensamma operationer som baserar sig på samtycke från en territorialstat och som territorialstaten själv inte deltar i. Om en gemensam operation däremot genomförs på en tredje stats territorium, ska på de metoder för underrättelseinhämtning som skyddspolisen använder tillämpas det som föreskrivs om underrättelseinhämtning som avser utländska förhållanden.

En polisman inom skyddspolisen som deltar i en gemensam operation utomlands lyder under skyddspolisen och dess interna och externa kontroll och omfattas av samma rättigheter och skyldigheter som inom annan underrättelseinhämtning som avser utländska förhållanden.

Enligt första meningen i 3 mom. i paragrafen ska chefen för skyddspolisen besluta om deltagande i internationellt samarbete och om användning av metoderna för underrättelseinhämtning. Avvikande från beslutet om deltagande i gemensamma operationer, vilket alltså grundar sig enbart på denna paragraf, tillämpas det som föreskrivs i 39 § på beslut om användning av metoder för underrättelseinhämtning vid gemensamma operationer utomlands.

Beslutet om deltagande i en gemensam operation ska grunda sig på behovet av att skydda den nationella säkerheten i Finland. En gemensam operation som utförs tillsammans med en annan stat på denna stats territorium ska således åtminstone indirekt ha en beröringsyta med skyddet av den nationella säkerheten i Finland. Det kan vara fallet till exempel om det är nödvändigt att få uppgifter om verksamheten i en terroristgrupp med aktivitet på en annan stats territorium och man antar att gruppens verksamhet påverkar eller kommer att påverka den nationella säkerheten i Finland.

I fråga om beslut om att lämna och begära internationellt bistånd finns särskilda bestämmelser i lagen om beslutsfattande om lämnande av och begäran om internationellt bistånd (418/2017).

I andra meningen i 3 mom. föreskrivs att en främmande stats behöriga tjänsteman har genom beslut av chefen för skyddspolisen rätt att på finskt territorium för att skydda den nationella säkerheten agera i samarbete med skyddspolisen och under handledning och övervakning av en polisman vid skyddspolisen använda sådana metoder för underrättelseinhämtning om vars användning beslut fattas i enlighet med bestämmelserna i 9, 10, 18, 20 och 24 §.

I motsats till första meningen i 4 mom. ges här en främmande stats tjänsteman genom beslut av chefen för skyddspolisen rätt att delta i gemensamma operationer på finskt territorium. Också beslutet om att en främmande stats tjänsteman får använda vissa i momentet särskilt föreskrivna metoder för underrättelseinhämtning fattas av chefen för skyddspolisen. En främmande stats tjänsteman får delta i samarbete i Finland bara om det är tillåtet enligt lagstiftningen i den sändande staten. Den främmande statens tjänsteman ska samarbeta under skyddspolisens ansvar, bestämmanderätt och ledning och i enlighet med finsk lagstiftning. I Finland ska den främmande statens tjänsteman iaktta de anvisningar och föreskrifter som en polisman vid skyddspolisen meddelar samt följa de begränsningar som skyddspolisen ställer.

En främmande stats tjänsteman kan genom beslut av chefen för skyddspolisen ges tillstånd att använda systematisk observation (9 §), förtäckt inhämtande av information (10 §), täckoperation (18 §), bevisprovokation genom köp (20 §) och styrd användning av informationskällor (24 §). Dessa metoder för underrättelseinhämtning innebär bara obetydliga ingrepp i de grundläggande fri- och rättigheterna, och ingen av dem inkräktar på skyddet av förtroliga meddelanden. En främmande stats tjänsteman kan använda dessa metoder för underrättelseinhämtning under ledning och övervakning av en polisman vid skyddspolisen. Det är då skyddspolisen som ansvarar för den gemensamma informationsinhämtningen och de metoder för underrättelseinhämtning som används. Systematisk observation kan göras såväl i realvärlden som i datanätet. I synnerhet i samband med observationer i datanätet kan det behövas bistånd från en sådan tjänsteman i den främmande staten som har egenskaper eller kunskaper som skyddspolisen saknar, såsom språkkunskaper eller kännedom om kulturen, och som tjänstemän vid skyddspolisen inte har. Ett liknande behov av gemensam operation kan handla om förtäckt inhämtande av information, täckoperation, bevisprovokation genom köp och styrd användning av informationskällor. Det är då fråga om att den främmande statens tjänsteman har en bistående roll i skyddspolisens informationsinhämtningsoperation. Utländska tjänstemän kan ha sådana kunskaper eller andra egenskaper som finländska tjänstemän saknar och som behövs för att operationen i fråga ska lyckas.

Enligt 4 mom. i paragrafen får skyddspolisen trots sekretessbestämmelserna överlåta information vid internationellt samarbete, om överlåtandet av informationen behövs för att skydda den nationella säkerheten och överlåtandet inte strider mot ett nationellt intresse. Överlämnandet av information enligt momentet ska först och främst grunda sig på skyddspolisens uppgift att skydda den nationella säkerheten. I praktiken kan det vara fråga om teknik och taktik som gäller metoderna för underrättelseinhämtning, uppgifter om skadliga program eller analyser av säkerhetsrisker eller annan sådan information som inte strider mot ett nationellt intresse. Överlämnande av information ska å andra sidan alltid tillgodose ett nationellt intresse. Exempel på sådan information är bland annat uppgifter om Finlands politiska eller ekonomiska förbindelser med en annan stat, uppgifter om militär underrättelseinhämtning eller militärt försvar eller uppgifter som tryggar det internationella underrättelsesamarbetet. Hur godtagbart överlämnandet av informationen är bör således bedömas med tanke på dels skyddet av den nationella säkerheten, dels tryggandet av internationella intressen. I denna samlade bedömning är det viktigt att beakta också egenskaperna hos den information som överlämnas och den instans som är mottagare av informationen.

Nödvändiga anteckningar om överlämnandet av information ska alltid göras för att möjliggöra en rättslig efterhandstillsyn.

Enligt 5 mom. finns det bestämmelser om utlämnande av personuppgifter i lagen om behandling av personuppgifter i polisens verksamhet. På utlämningen av personuppgifter i det internationella samarbetet tillämpas således den lagen och inte 5 mom. i denna paragraf.

58 §. *Samordning av underrättelseverksamheten.* I 1 mom. i paragrafen föreskrivs om samordning av underrättelseinhämtning. Enligt 1 mom. ska den civila och den militära underrättelseverksamheten samordnas mellan republikens president, statsrådets kansli, utrikesministeriet, försvarsministeriet och inrikesministeriet samt vid behov andra ministerier och myndigheter.

Utrikes- och säkerhetspolitiska ministerutskottet har som uppgift att i förberedande syfte behandla viktiga utrikes- och säkerhetspolitiska frågor och andra frågor som gäller Finlands relationer till utländska stater, anknytande viktiga frågor om den inre säkerheten samt viktiga frågor som gäller landets totalförsvar liksom frågor om samordningen av dessa.

I momentet nämns förutom republikens presidents och statsrådets organisation också de myndigheter som möjliggör en förberedande samordning av underrättelseverksamheten med stöd av en bredare expertis till exempel i en grupp för samordning av underrättelseinhämtning och lägesbilder. I gruppen ingår bland annat underrättelsechefen för huvudstaben och chefen för skyddspolisen. Dessutom finns det möjlighet att vid behov utse representanter för andra ministerier och myndigheter.

Genom samordning av underrättelseinhämtningen säkerställs i fråga om informationshanteringen reaktionerna på utrikes- och säkerhetspolitiska begäranden om information som är viktiga med tanke på underrättelseinhämtningen, beaktandet av olika förvaltningsområdens synpunkter på underrättelseverksamheten och förmedlingen av dessa synpunkter som framkommit i processen till behöriga instanser. Vid samordning är det funktionellt fråga om att peka på och koordinera prioriteterna inom informationshämtningen och fördela uppgifterna inom underrättelseverksamheten mellan civil och militär underrättelseinhämtning på basis av en ändamålsenlighetsprövning av underrättelseobjektet och hotets karaktär. I samband med prövningen är det möjligt att bedöma exempelvis utrikespolitiska svagheter och influenser på Finlands internationella förbindelser med eventuell anknytning till civil och militär underrättelseinhämtning som genomförs någon annanstans än i Finland. Vid samordning av underrättelseverksamheten är det däremot inte fråga om övervakning av underrättelseinhämtning eller styrning som inbegriper den operativa verksamheten, såsom att använda en metod för underrättelseinhämtning för beslutsfattande.

Om det bedöms att den civila underrättelseverksamheten har utrikes- och säkerhetspolitiska konsekvenser, ska ärendet enligt 2 mom. i förberedande syfte behandlas mellan de myndigheter som nämns i 1 mom. Också för närvarande bereder de myndigheter som avses i 1 mom. viktiga utrikes- och säkerhetspolitiska frågor tillsammans innan dessa lämnas till utrikes- och säkerhetspolitiska ministerutskottet för behandling. Uppgiften överlappar dock inte ministerutskottets uppgift, utan den process som avses i momentet är en åtgärd som föregår utskottsbehandlingen och syftar till att göra ministerutskottets behandling smidigare och säkerställa en sammanhängande behandling.

I 17 § i lagen om militär underrättelseverksamhet föreslås en samordning av underrättelseverksamheten på samma sätt som i denna paragraf.

59 §. *Inrikesförvaltningens övervakning av den civila underrättelseinhämtningen.* I paragrafen föreskrivs om den civila underrättelseinhämtningens interna övervakning av skyddspolisen. Enligt paragrafen övervakas den informationsinhämtning som avses i detta kapitel av chefen för skyddspolisen och av inrikesministeriet.

60 §. *Extern övervakning av den civila underrättelseinhämtningen*. Enligt 1 mom. i paragrafen ska inrikesministeriet årligen lämna en berättelse till riksdagens justitieombudsman om hur de i detta kapitel avsedda metoderna för underrättelseinhämtning har använts och användningen övervakats samt hur det i detta kapitel avsedda skyddandet av den civila underrättelseinhämtningen har använts och användningen övervakats. Övervakningen av hur de har använts ska omfatta både användningen av metoder för underrättelseinhämtning och användningen av skyddandet av den civila underrättelseinhämtningen. För att inrikesministeriet ska kunna lämna sin berättelse till riksdagens justitieombudsman krävs det att skyddspolisen på det sätt som inrikesministeriet anger lämnar ministeriet de uppgifter som behövs för att utarbeta en berättelse.

I 2 mom. ingår en hänvisningsbestämmelse till lagen om övervakning av underrättelseverksamheten. Hänvisningsbestämmelsen är motiverad eftersom underrättelseombudsmannens laglighetsövervakning och riksdagens parlamentariska övervakning är de viktigaste elementen i övervakningen av underrättelseverksamheten.

61 §. *Anmälningar till underrättelseombudsmannen*. Enligt 1 mom. i paragrafen ska skyddspolisen informera underrättelseombudsmannen om de tillstånd och beslut som gäller användning av en metod för underrättelseinhämtning och som har meddelats med stöd av detta kapitel så snart som möjligt efter det att tillståndet beviljades eller beslutet fattades.

För att säkerställa att övervakningen av underrättelseverksamheten sker i realtid är det ändamålsenligt att skyddspolisen som civil underrättelsemyndighet gör en anmälan om tillstånd eller beslut som gäller underrättelseinhämtningsmetoder till underrättelseombudsmannen. Anmälningsskyldigheten ska också inbegripa domstolens negativa beslut om så kallade brådskande beslut samt de tillstånd och negativa beslut som domstolen beviljat enligt 16 § 2 mom. I praktiken fullgörs informationsskyldigheten genom att man skickar en kopia av det tillstånd som beviljats av domstolen eller det beslut som fattats av skyddspolisen till underrättelseombudsmannen. Samtidigt kan också ett yrkande av domstolen som gäller tillståndsärendet lämnas till underrättelseombudsmannen.

Anmälningen spelar också en viktig roll för den externa övervakningen av användningen av metoderna för underrättelseinhämtning. Underrättelseombudsmannen behöver ha aktuell information om vilken typ av befogenheter skyddspolisen utövar inom den civila underrättelseinhämtningen. Underrättelseombudsmannen ska övervaka bland annat att skyddspolisen håller sig inom de gränser som det av domstolen beviljade tillståndet förutsätter.

Det är viktigt att underrättelseombudsmannen får information särskilt om andra beslut än de tillstånd som beviljats av domstolen. Det är av största vikt att en oberoende rättslig kontroll är möjlig i sådana här frågor eftersom det, i motsats till när domstolen beviljar tillstånd, inte har gjorts någon extern objektiv bedömning av de beslut som underrättelsemyndigheten själv har fattat innan underrättelseinhämtningsmetoden tas i bruk.

I 2 mom. föreskrivs om andra anmälningar till underrättelseombudsmannen än de som avses i 1 mom. Skyddspolisen ska så snart som möjligt informera underrättelseombudsmannen om ett beslut som gäller 1) skyddande av civil underrättelseverksamhet (36 §), 2) yppandeförbud (38 §) och 3) uppskjutande av en anmälan enligt 44 § 1 mom.

Enligt 3 mom. i paragrafen ska det vid underrättelse om ett beslut som gäller en metod för underrättelseinhämtning fästas särskild vikt vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.

Användningen av metoder för underrättelseinhämtning och besluten om dessa innehåller information som till sin karaktär är mycket känslig och sekretessbelagd. I samband med de anmälningar som avses i paragrafen ska man fästa särskild vikt vid att sekretessen iakttas och informationssäkerheten tryggas. Anmälan till underrättelseombudsmannen ska göras så att det inte finns någon risk för att den sekretessbelagda informationen röjs. De uppgifter som är föremål för anmälan ska behandlas bara i sådana utrymmen som i fråga om utrymmes- och konstruktionssäkerhet är sådana att det är tryggt och säkert att behandla uppgifter i dem utan att det finns risk för att uppgifterna röjs.

Om anmälningsskyldigheten genomförs med hjälp av automatisk databehandling, ska dataöverföringen vara sådan att den i sig inte medför risk för att den sekretessbelagda informationen röjs. Åtminstone när det gäller andra anmälningar än de som avses i 1 mom. är det motiverat att man gör sig förtrogen med de beslut som anmälan grundar sig på i underrättelsemyndighetens utrymmen. Ett beslut ska kunna anmälas med hjälp av en sådan kommunikationsutrustning som till sina tekniska egenskaper gör det möjligt att ge bara underrättelseombudsmannen tillgång till informationen.

Anmälningsförfarandet ska inte i sig medverka till att det blir en klar obalans mellan kostnaderna för förfarandet och syftet med den anmälan som görs till underrättelseombudsmannen.

62 §. *Bemyndigande att utfärda förordning.* I paragrafen föreskrivs om sådana omständigheter som kan regleras genom förordning av statsrådet eller inrikesministeriet.

Enligt 1 mom. får det genom förordning av statsrådet utfärdas bestämmelser om 1) hur användningen av metoder för underrättelseinhämtning och skyddandet av dem ska ordnas, 2) dokumenteringen av åtgärderna för övervakningen, 3) de redogörelser som ska lämnas för övervakningen av den civila underrättelseinhämtningen, 4) det förfarande som gäller överföring av en uppgift som ska lämnas ut till brottsbekämpningen (44 § 1 mom.), 5) organiserandet av samarbetet mellan skyddspolisen och militärunderrättelsemyndigheten (54 §), 6) organiserandet av samarbetet mellan skyddspolisen och andra myndigheter (55 §), 7) organiserandet av samordningen av den hemliga informationsinhämtningen (56 §), 8) organiserandet av samordningen av underrättelseverksamheten (58 §).

I den civila och den militära underrättelselagstiftningen är det nödvändigt att genom förordning av statsrådet reglera de faktahelheter som avses i 1–4 punkten redan innan lagen träder i kraft.

Enligt 2 mom. i paragrafen får det genom förordning av inrikesministeriet utfärdas bestämmelser om 1) organiserandet av övervakningen av den civila underrättelseverksamheten inom inrikesförvaltningen (59 §), 2) organiserandet av samarbetet mellan skyddspolisen och den övriga inrikesförvaltningen, 3) organiserandet av skyddspolisens internationella samarbete (57 §).

Av alla bestämmelser om bemyndigande att utfärda förordning framgår det att de är begränsade till tekniska eller processuella förfaranden. Till exempel 1 mom. 1–4 punkten i bemyndigandet har i sak samma innehåll som bestämmelserna i 4 kap. 65 § i polislagen och 10 kap. 67 § i tvångsmedelslagen.

Med hänsyn till frågornas karaktär är det motiverat med bestämmelser i förordning, eftersom det inte är fråga om individens rättigheter och skyldigheter, då frågan bör regleras genom lag, utan om att ordna myndigheternas interna verksamhet eller verksamheten mellan myndigheterna.

9 kap. **Särskilda bestämmelser**

8 §. *Begränsningar i rätten att färdas och vistas i ett område.* I paragrafen görs en teknisk justering så att det finska namnet på inrikesministeriet, sisäasiainministeriö, ändras till sisäministeriö.

9 §. *Internationellt samarbete*. I 2 mom. i paragrafen görs en teknisk justering så att det finska namnet på inrikesministeriet, sisäasiainministeriö, ändras till sisäministeriö.

10 §. *Närmare bestämmelser.* I 1 mom. i paragrafen görs en teknisk justering så att det finska namnet på inrikesministeriet, sisäasiainministeriö, ändras till sisäministeriö.

1.2 Lag om civil underrättelseinhämtning avseende datatrafik

1 §. *Tillämpningsområde och förhållande till annan lagstiftning.* Paragrafen gäller lagens tillämpningsområde och förhållande till övrig lagstiftning.

Enligt 1 mom. innehåller lagen bestämmelser om användning av underrättelseinhämtning som avser datatrafik vid sådan civil underrättelseinhämtning som avses i 5 a kap. i polislagen (872/2011). Med civil underrättelseinhämtning avses enligt 1 § i det föreslagna 5 a kap. i polislagen skyddspolisens inhämtande och nyttjande av information för att den nationella säkerheten ska kunna skyddas och den högsta statsledningens beslutsfattande stödjas samt för att andra myndigheter ska kunna utföra de lagstadgade uppgifter som hänför sig till den nationella säkerheten . Bestämmelser om föremål för den civila underrättelseinhämtningen ska enligt förslaget ingå i 5 a kap. 3 § i polislagen och i 3 § i denna lag. Bestämmelserna är enligt förslaget likalydande. Eftersom man med civil underrättelseinhämtning enligt 5 a kap. 1 § i polislagen avser endast sådant inhämtande av information som utförs av skyddspolisen, är det bara skyddspolisen som kan använda sådan underrättelseinhämtning som avses i denna lag. Detta framgår också av de föreslagna 7, 9 och 10 §.

Paragrafens 2 mom. har informativ karaktär. Enligt den första meningen ska bestämmelser om användningen av underrättelseinhämtning som avser datatrafik i militär underrättelseinhämtning och om det tekniska genomförandet av den underrättelseinhämtning som avser datatrafik ingå i lagen om militär underrättelseverksamhet. Syftet med meningen är att regleringen av den underrättelseinhämtning som avser datatrafik ska ske såväl genom denna som genom en annan lag. Föremålen för den underrättelseinhämtning avseende datatrafik som används i den militära underrättelseinhämtningen bestäms enligt lagen om militär underrättelseverksamhet, och de är delvis andra än föremålen för underrättelseinhämtning enligt denna lag. Men lagen om militär underrättelseverksamhet ska också innehålla bestämmelser om det tekniska genomförandet av den underrättelseinhämtning som avser datatrafik vilka kompletterar denna lag. Enligt 10 § i denna lag ska försvarsmaktens underrättelsetjänst på uppdrag av skyddspolisen svara för det tekniska genomförandet av den underrättelseinhämtning som avser datatrafik. I denna roll ska försvarsmaktens underrättelsetjänst förutom 10 § i denna även tillämpa de bestämmelser om det tekniska genomförandet som ingår i lagen om militär underrättelseverksamhet. Till dessa hör bland andra 66, 72 och 73 §.

Enligt den andra meningen i momentet ska det föreskrivas om teleavlyssning som används vid civil underrättelseinhämtning, inhämtande av information i stället för teleavlyssning samt te-

leövervakning i 5 a i polislagen. Den underrättelseinhämtning som avser datatrafik påminner om de metoder för underrättelseinhämtning som regleras i polislagen såtillvida att det även i dessa är fråga om underrättelseinhämtning som gäller elektronisk kommunikation. Skillnaden är den att underrättelseinhämtning som avser datatrafik inte som de sist nämnda metoderna ska riktas mot någon teleadress eller teleterminalutrustning som kan specificeras på förhand för att följa en bestämd persons kommunikation. Huruvida man vid inhämtandet av information ska använda underrättelseinhämtning som avser datatrafik eller de metoder som anges i 5 a kap. i polislagen ska bestämmas enligt 6 § 2 mom. Enligt bestämmelsen är en förutsättning för att underrättelseinhämtning som avser datatrafik ska få företas att den är nödvändig. Nödvändighetskriteriet innebär att underrättelseinhämtning som avser datatrafik får användas bara om information inte kan inhämtas eller om inhämtandet är oskäligt besvärligt på annat sätt. Om identifieringsuppgifterna för en teleterminalutrustning eller en teleadress är kända för en myndighet för civil underrättelseinhämtning och det inte av andra orsaker är mycket svårt att använda de metoder för underrättelseinhämtning som avses i 5 a kap. i polislagen, uppfylls inte kravet i den föreslagna lagen om att underrättelseinhämtning som avser datatrafik ska vara nödvändig. Kravet om nödvändighet ska emellertid inte innebära en jämförelse med enbart möjligheterna att inhämta informationen genom de metoder för underrättelseinhämtning som nämnts ovan, utan även möjligheterna att skaffa dem med andra metoder som nämns i det föreslagna 5 a kap. i polislagen ska beaktas.

I paragrafens 3 mom. konstateras det att bestämmelser om behandlingen av information som erhållits genom underrättelseinhämtning som avser datatrafik förutom i denna lag även ska ingå i lagen om behandling av personuppgifter i polisens verksamhet (761/2003). Bara de bestämmelser om behandling av personuppgifter som är nödvändiga ska enligt förslaget tas med i lagen. Till dessa hör bestämmelser om förbud mot underrättelseinhämtning som begränsar underrättelseinhämtning som avser datatrafik (12 § i den föreslagna lagen), om granskning av de upptagningar och handlingar som uppkommit vid underrättelseinhämtning som avser datatrafik (13 §), om undersökning av upptagningarna (14 §), om skyldigheten att utan dröjsmål utplåna en del av den information som uppkommit genom underrättelseinhämtning som avser datatrafik (15 §) och om utlämning av information som uppkommit genom underrättelseinhämtning som avser datatrafik för brottsbekämpning (17 §). Den föreslagna lösningen liknar till exempel den som ingår i 5 kap. i den nuvarande polislagen. I andra avseenden än dem som nämns ovan ska det föreskrivas om behandlingen av personuppgifter i lagen om behandling av personuppgifter i polisens verksamhet som är den allmänna lag som ska tillämpas på automatisk behandling av personuppgifter och annan behandling av personuppgifter som behövs när de uppgifter som avses i 1 kap. 1 § i polislagen utförs. Att behandlingen av information som inhämtats genom underrättelseinhämtning som avser datatrafik ska regleras i lagen om behandling av personuppgifter i polisens verksamhet motiveras av att det finns behov att jämföra och analysera sådana uppgifter tillsammans med uppgifter som skaffats genom andra metoder för underrättelseinhämtning för att kunna förstå hur relevanta de är och för att förstå sammanhanget. Information som uppkommer som ett resultat av en sådan analys av flera källor kan inte anses vara ren information från underrättelseinhämtning som avser datatrafik, varför det inte heller är ändamålsenligt att föreskriva om den i lagen om civil underrättelseinhämtning avseende datatrafik.

2 §. *Definitioner.* Paragrafen innehåller definitionerna av de centrala begrepp som används i lagen.

Enligt 1 punkten avses med underrättelseinhämtning som avser datatrafik tekniskt inhämtande av information som utförs på datatrafik över Finlands gräns i kommunikationsnätverk och grundar sig på automatiserad avskiljning av data samt behandling av denna information. De väsentliga elementen i definitionen är för det första att underrättelseinhämtningen gäller datatrafik över Finlands gräns, för det andra att gränsen överskrids i ett kommunikationsnät och

för det tredje att underrättelseinhämtning som avser datatrafik till sin karaktär är ett tekniskt inhämtande av information som grundar sig på automatiserad avskiljning.

Att datatrafiken överskrider Finlands gräns innebär att den de facto överskrider statsgränsen genom att övergå från ett finskt kommunikationsnät till ett utländskt eller vice versa. Tekniskt genomförs underrättelseinhämtningen så nära de ställen som möjligt där det finska kommunikationsnätet och det fasta utländska nätet eller satellitnätet är hopkopplade och trafiken över gränsen följaktligen sker. Det sker alltså i regel så nära den länk som går över statsgränsen som möjligt. Placeringen kan likväl vara längre från länken om det är ändamålsenligt med hänsyn till verksamheten hos den dataöverförare som definieras i 3 punkten.

Eftersom även datakommunikation som är avsedd att ske inom Finlands gränser på grund av internets karaktär slumpmässigt kan styras via ett utländskt kommunikationsnät, omfattas även sådan datatrafik i princip av definitionen. För att säkerställa att man trots detta inte genom underrättelseinhämtning som avser datatrafik inhämtar information från trafik som till sin faktiska natur är inhemsk, föreslås det i 12 § ett förbud mot informationsinhämtning vad gäller inhemsk kommunikation och i 15 § en skyldighet att utplåna sådan information.

När datatrafiken överskrider gränsen, ska det ske i ett kommunikationsnät. I 2 punkten föreslås det att begreppet kommunikationsnät definieras på ett sätt som begränsar vilka nät den underrättelseinhämtning som avser datatrafik kan gälla.

Till definitionen av underrättelseinhämtning som avser datatrafik hör att det är fråga om tekniskt inhämtande av information som grundar sig på automatisk avskiljning och om behandling av informationen. I detta hänseende är syftet att särskilja underrättelseinhämtning som avser datatrafik från andra sätt att inhämta information ur datatrafik i kommunikationsnät och då framför allt från teleavlyssning och teleövervakning. Vid teleavlyssning och teleövervakning kan insamlingen av information genomföras så nära den enskilda teleadress eller teleterminalutrustning som är föremål för åtgärden som möjligt. Vid underrättelseinhämtning som avser datatrafik är det inte fråga om sådant inhämtande av information som gäller en enskild teleterminalutrustning eller teleadress utan om avskiljning av datatrafik med automatiserade metoder på ett sådant ställe i datanätet där man kan anta att en så stor del som möjligt av den datatrafik som är föremålet för underrättelseinhämtningen passerar. I praktiken genomförs avskiljandet så att datatrafiken jämförs med sökbegrepp, det vill säga kriterier som valts på förhand. Ett av syftena med den underrättelseinhämtning som avser datatrafik är enligt förslaget att identifiera enskilda teleterminaler och teleadresser för att göra teleavlyssning och teleövervakning möjlig. Bestämmelser om det praktiska genomförandet av den automatiserade avskiljningen ska enligt förslaget finnas i 4 §.

Enligt definitionen ska underrättelseinhämtning som avser datatrafik förutom tekniskt inhämtande av information baserad på automatiserad avskiljning även innefatta behandling av inhämtad information. Med behandling av den inhämtade informationen avses såväl automatisk som manuell behandling av den automatiskt avskilda informationen. Om denna föreskrivs det i den föreslagna 5 §.

I 2 punkten definieras begreppet kommunikationsnät. Begreppet är viktigt därför att underrättelseinhämtning som avser datatrafik enligt definitionen i 1 punkten kan gälla bara sådan datatrafik som överskrider Finlands gräns i ett kommunikationsnät. Med kommunikationsnät avses liksom i 3 § 39 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) ett system som består av sammankopplade ledningar och av anordningar och som är avsett för överföring eller distribution av meddelanden via ledning, med radiovågor, optiskt eller på något annat elektromagnetiskt sätt. Väsentligt i definitionen är för det första att systemet är avsett för överföring eller distribution av meddelanden. Eftersom ett av kriterierna i definitionen

är användningsområdet kan man genom underrättelseinhämtning som avser datatrafik även granska sådan datatrafik i ett kommunikationsnät som eventuellt inte ska anses som kommunikation. För det andra ingår det i definitionen ett krav på systemets tekniska elektromagnetiska utförande. Kravet är i övrigt teknologineutralt. Inom definitionen faller de system där överföringen eller distributionen sker via ledning, med radiovågor, optiskt eller på något annat sätt, förutsatt att det är elektromagnetiskt.

I 3 punkten definieras begreppet dataöverförare. Med dataöverförare avses en aktör som äger eller kontrollerar en sådan del av ett kommunikationsnät som överskrider Finlands gräns. Definitionen har betydelse när man ska säkerställa att skyldigheterna enligt den aktuella lagen och lagen om militär underrättelseverksamhet att medverka i genomförandet av underrättelseinhämtning som avser datatrafik åläggs rätt aktörer. Till dessa skyldigheter hör för det första dataöverförarens skyldighet enligt 22 § i lagen att utan ogrundat dröjsmål till skyddspolisen överlämna sådan information som behövs för att specificera en del av kommunikationsnätet med tanke på ett krav för att få tillstånd att använda underrättelseinhämtning som avser datatrafik och beslut om ett sådant tillstånd. För det andra är det fråga om en skyldighet avsedd att säkerställa att man i en del av ett kommunikationsnät som överskrider landets gräns, det vill säga praktiska sett i datakommunikationsförbindelsen, kan installera en så kallad anslutningspunkt det vill säga en anslutning genom vilken underrättelseinhämtningen genomförs. I 94 § i lagen om militär underrättelseverksamhet ska det föreskrivas om dataöverförarens skyldighet att bistå vid inrättandet av en anslutningspunkt som behövs för underrättelseinhämtning som avser datatrafik genom att ge försvarsmaktens underrättelsetjänst information som behövs för detta ändamål samt tillgång till de utrymmen där anslutningspunkten ska placeras. Bestämmelser om dataöverförarens skyldighet att bistå vid inrättandet av anslutningen ska enligt förslaget ingå i lagen om militär underrättelseverksamhet därför att frågan har nära samband med det tekniska genomförandet av den underrättelseinhämtning som avser datatrafik. Den reglering som möjliggör byggandet av anslutningen kommer emellertid att bidra till att tillgodose behov inom den civila underrättelseinhämtning som avser datatrafik.

Begreppet dataöverförare innefattar såväl ägare till sådana delar av ett kommunikationsnät som överskrider gränsen som innehavare av sådana delar. Med innehavare avses ett sådant finskt eller utländskt företag eller en sådan finsk eller utländsk sammanslutning som de facto kontrollerar den del av kommunikationsnätet som överskrider gränsen till exempel efter att ha hyrt den av företaget eller sammanslutningen som äger den för att driva den som operatör. Dataöverföraren är således den aktör som har de tekniska förutsättningarna för att bestämma i vilken del av kommunikationsnätet en viss datatrafik sker. Ur en informationsteknisk synvinkel är dataöverföraren den aktör som styr nättrafiken vad gäller de två lägsta skikten i den så kallade OSI-referensmodellen (Open Systems Interconnection Reference Model), det vill säga på det fysiska skiktet och datalänkskiktet. Begreppet dataöverförare omfattar följaktligen inte sådana företag eller sammanslutningar som har hyrt dataöverföringskapacitet av dataöverförare utan att ha datatekniska möjligheter att självständigt påverka i vilken del av nätet någon del av datatrafiken sker. På grund av begränsningen ovan bedömer man att högst ett tiotal företag för närvarande faller inom den föreslagna definitionen på dataöverförare. Det finns skäl att betona att definitionen på dataöverförare inte motsvarar definitionen på kommunikationsförmedlare i 3 § 36 punkten i lagen om tjänster inom elektronisk kommunikation, utan att den är mycket snävare.

3 § *Föremål för underrättelseinhämtning som avser datatrafik.* I paragrafen föreskrivs det på ett uttömmande sätt om de objekt om vilka uppgifter får inhämtas genom underrättelseinhämtning som avser datatrafik. Underrättelseinhämtning som avser datatrafik får inte användas för inhämtande av uppgifter om sådana omständigheter, fenomen eller hot som inte nämns särskilt i paragrafen.

Eftersom föremålen för civil underrättelseinhämtning, vilka är de samma som föremålen för underrättelseinhämtning som avser datatrafik om vilka det även föreskrivs på motsvarande sätt som i 5 a kap. 3 § i polislagen, hänvisar vi när det gäller motiveringarna till denna paragraf till motiveringarna till den paragrafen.

4 §. *Förutsättningar för användning av underrättelseinhämtning som avser datatrafik.* I paragrafen föreskrivs det om villkoren för användning av underrättelseinhämtning som avser datatrafik.

Enligt 1 mom. är ett allmänt villkor för användning av underrättelseinhämtning som avser datatrafik att man med den med fog kan antas få information om sådan verksamhet som är föremål för underrättelseinhämtning som avser datatrafik och som allvarligt hotar den nationella säkerheten. Det är fråga om ett krav på grundad resultatförväntan, som ska tillämpas på all underrättelseinhämtning som avser datatrafik. Om man genom underrättelseinhämtningen inte över huvud taget kan väntas få information om verksamhet som innebär ett allvarligt hot mot den nationella säkerheten, det vill säga om underrättelseinhämtningen inte kan antas bli resultatrik, ska den inte få användas.

När man jämför paragrafens 1 och 2 mom. med varandra observerar man att det för sådan underrättelseinhämtning avseende datatrafik som kan riktas uteslutande mot en främmande stats datatrafik inte ställs andra villkor än att underrättelseinhämtningen ska leda till resultat. Det anses inte motiverat att ställa striktare villkor än dessa, eftersom staten och andra offentliga samfund inte omfattas av skyddet för de grundläggande fri- och rättigheterna (RP 309/1993 och GrUU 9/2015). Följaktligen gäller skyddet för hemligheten i fråga om förtroliga meddelanden inte kommunikation eller annan datatrafik från en främmande stats myndighetsorganisation.

I momentet nämns förutom en främmande stat även en aktör som är jämställbar med en främmande stat. Innebörden av detta behandlas närmare i motiveringarna till 5 a kap. 4 § 4 mom. i polislagen. Bestämmelser om underrättelseinhämtning som riktas mot en statlig aktörs datatrafik ingår i 66 och 67 § i lagen om militär underrättelseverksamhet.

En tillämpning av enbart resultatförväntan enligt 1 mom. förutsätter i praktiken att en främmande stats eller med en sådan jämställbar aktörs datatrafik som sökbegrepp tillämpas på sker separat från övrig datatrafik i kommunikationsnätet. Det är alltså fråga om en situation där den automatiska jämförelse som utförs med hjälp av sökbegrepp omfattar enbart statlig datatrafik till exempel därför att den sker i en del av kommunikationsnätet som reserverats för denna trafik. Om den främmande statens eller därmed jämförbara aktörens datatrafik är blandad med annan datatrafik så att användningen av sökbegrepp skulle omfatta båda, ska man utöver kravet på resultatförväntan i 1 mom. även tillämpa det nödvändighetsvillkor som anges i det föreslagna 2 mom.

Om användningen av sökbegrepp för underrättelseinhämtning som avser datatrafik inte gäller enbart en främmande stats eller därmed jämförbar aktörs datatrafik är ett villkor enligt 2 mom. dessutom att underrättelseinhämtningen kan antas vara nödvändig på grund av den verksamhet som är föremål för underrättelseinhämtningen och som utgör ett allvarligt hot mot den nationella säkerheten. I detta avseende ställs det strängare krav än på de metoder för underrättelseinhämtning enligt det föreslagna 5 a kap. i polislagen som ingriper i skyddet av konfidentiella meddelanden. En bakgrund till denna lösning finns i Europadomstolens avgörande i fallet Szabo och Vissy mot Ungern, enligt vilket villkoret om nödvändighet i ett demokratiskt samhälle i artikel 8 i människorättskonventionen i samband med en övervakningsteknik av det slag som underrättelseinhämtning som avser datatrafik utgör ska tolkas så att det förutsätter ”absolut nödvändighet” (strict necessity). Användningen av metoden ska på ett allmänt plan

vara absolut nödvändig för att skydda de demokratiska institutionerna. För det andra ska användningen av metoden i samband med en enskild underrättelseinhämtningsoperation vara absolut nödvändig för att inhämta synnerligen viktig information (vital information).

Med den nödvändighet som föreslås som villkor för användningen av underrättelseinhämtning som avser datatrafik förstås att användningen är en sistahandsåtgärd, det vill säga att inhämtande av information på annat sätt inte är möjligt eller exempelvis skulle kräva väsentligt mera resurser eller fördröja underrättelseinhämtningen. I överensstämmelse med de kriterier för prövning av nödvändigheten som anges i regeringens proposition om översyn av tvångsmedelslagen (RP 222/2010 rd, s. 326) ska det likväl inte krävas en utredning grundad på faktisk användning av eller försök att använda andra metoder för underrättelseinhämtning, eftersom man då skulle bli tvungen att genomföra dyra och onödiga åtgärder som inkräktar på skyddet för privatlivet. Nödvändigheten kan grunda sig på en helhetsbedömning som visar att andra metoder till exempel skulle vara resultatlösa eller inte lämpa sig för inhämtande av informationen utan att man konkret skulle ha försökt använda dem. Tillämpningen av bestämmelsen förutsätter jämförelse mellan de metoder för underrättelseinhämtning som anges i det föreslagna 5 a kap., särskilt teleavlyssning och teleövervakning, och underrättelseinhämtning som avser datatrafik. Eftersom teleavlyssning och teleövervakning i regel kan inriktas exaktare än underrättelseinhämtning som avser datatrafik, innebär användningen av teleavlyssning och teleövervakning mindre risk för att utomståendes kommunikation blir utsatt för underrättelseverksamheten. Om användning av teleavlyssning eller teleövervakning i ett enskilt fall inte är omöjlig eller mycket besvärlig, ska de användas som primära metoder som används hellre än underrättelseinhämtning som avser datatrafik.

I lagförslaget har nödvändighetskravet inte i någon bestämmelse konkretiserats med ett krav om att de uppgifter som den underrättelseinhämtning som avser datatrafik resulterar i är synnerligen viktig. Detta beror på att prövningen huruvida en uppgift är synnerligen viktig är svårare vid underrättelseinhämtning än vid brottsbekämpning, där det handlar om att förhindra, avslöja eller utreda en konkret handling. Ställer man kravet att en uppgift som fås genom underrättelseinhämtning som avser datatrafik ska vara synnerligen viktig, kan kravet tolkas så att uppgiften ska vara nödvändig för att avvärja en fara som omedelbart hotar den nationella säkerheten. Vid underrättelseinhämtning, särskilt underrättelseinhämtning som avser datatrafik, är det likväl inte enbart fråga om att avvärja omedelbara faror utan det handlar även om mera långsiktigt inhämtande av information om verksamheter som allvarligt hotar den nationella säkerheten. Underrättelseinhämtning som avser datatrafik kan vara nödvändig för att inhämta sådan information som i följande skede möjliggör användningen av någon av de metoder för underrättelseinhämtning som avses i 5 a kap. i polislagen men som inte skilt för sig kan anses nödvändig för att avvärja ett hot. Den civila underrättelseinhämtningen avses innefatta olika metoder att inhämta information som kompletterar varandra och bildar en helhet inom ramen för vilken det är mycket svårt att på förhand bedöma och påvisa betydelsen av den information som varje enskild metod kan bidra med till en helhetsuppfattning av den verksamhet som är föremål för informationsinhämtningen.

5 § *Inriktande av underrättelseinhämtning som avser datatrafik.* I paragrafen föreskrivs det om hur underrättelseinhämtningen som avser datatrafik ska inriktas, det vill säga hur datatrafik som sammanhänger med verksamhet som allvarligt hotar den nationella säkerheten ska identifieras och styras till fortsatt behandling enligt 6 §.

Enligt 1 mom. i paragrafen ska underrättelseinhämtning som avser datatrafik inriktas med hjälp av automatiserad avskiljning av datatrafiken som baserar sig på användning av sökbegrepp. Sökbegrepp ska användas bara på datatrafik som äger rum i en bestämd del av kommunikationsnätet. Denna del bestäms av en domstol i ett tillståndsbeslut enligt 7 § eller i undantagsfall av skyddspolisens chef i ett tillfälligt, brådskande beslut enligt 9 §. Den datatrafik som

går genom delen i fråga speglas och leds genom underrättelsesystemet, där systemet jämför datatrafiken med de sökbegrepp som matats in i systemet på förhand. Jämförelsen utförs tekniskt, varför ingen fysisk person ser de data som strömmar genom systemet. Endast sådan datatrafik som motsvarar sökbegreppen styrs till den fortsatta behandling enligt 6 § som är följande behandlingsfas i underrättelseinhämtningen. Data som inte motsvarar sökbegreppen passerar genom systemet och kan inte granskas på nytt i ett senare skede. Den automatiserade avskiljning som utförs med hjälp av sökbegrepp utgör det tekniska genomförandet av den underrättelseinhämtning som avser datatrafik. Enligt 10 § är det försvarsmaktens underrättelsetjänst som ska sköta detta också för skyddspolisens del.

I 2 mom. anges sökbegreppens karaktär. Enligt den huvudregel som framgår av momentet får sökbegreppet inte beskriva innehållet i ett meddelande. Med innehållet i ett meddelande avses det semantiska innehåll i meddelandet som avsändaren sänt mottagaren. På grund av förbudet får sökbegreppet inte beskriva till exempel uttryck som de kommunicerande personerna använder eller personers namn eller andra identifieringsuppgifter som ingår i meddelandet. Förbudet mot användning av sökbegrepp som beskriver innehållet ska även gälla innehållet i dokument eller filer som sparas i eller hämtas från molntjänster. Förbudet mot att använda sökbegrepp som gäller innehållet ska gälla alla andra fall än de där sökbegrepp jämförs endast med en främmande stats eller med en sådan jämställbar aktörs datatrafik eller där sökbegrepp beskriver innehållet i ett skadligt datorprogram eller datorkommando. Undantagen från förbudet är förknippade med sådana typer av datatrafik som inte kan anses omfattas av skyddet för konfidentiella meddelanden. Om det däremot är fråga om datatrafik som omfattas av skyddet för de grundläggande fri- och rättigheterna, är sökbegrepp som beskriver innehållet i ett meddelande över huvud taget inte tillåtna.

I de europeiska referensländer som lagstiftat om underrättelseinhämtning som avser datatrafik har det i den aktuella lagstiftningen inte angetts begränsningar av eller förbud mot användningen av sökbegrepp som beskriver innehållet av det slag som angetts ovan. Sökbegrepp som beskriver innehållet i meddelanden får användas i länderna i fråga. De föreslagna begränsningarna i användningen av sökbegrepp som beskriver innehållet är alltså en specifik lösning för Finland. Syftet är att i så hög grad som möjligt trygga kärnan i det skydd för hemligheten i fråga om förtroliga meddelanden som gäller utomstående personer.

På grund av förbudet mot sökbegrepp som beskriver innehållet får sökbegreppen bara beskriva styrdata för kommunikationen och annan sådan information som inte kan anses höra till det semantiska innehåll i meddelandet som avsändaren avsett för mottagaren. Till styrdata hör anvisningar, kommandon och andra metadata söm är avsedda för datanätet eller det sändande eller mottagande datasystemet och som används för att påverka hur meddelandet transporteras och styrs i nätet och datasystemet.

Vid underrättelseinhämtning som avser datatrafik avskiljs styrdata från meddelandets innehåll i applikationsskiktet i OSI-referensmodellen som beskriver nättrafikens funktion. Eftersom avskiljningen sker i programskiktet, ska som styrdata även betraktas uppgifter som används av programvaran i den mottagande anordningen för att styra meddelandet exakt till rätt mottagare. Ett exempel på sådana data som när frågan betraktas med hänsyn till applikationsskiktet inte behandlas som en del av meddelandets innehåll och som därför får användas som sökbegrepp är meddelandets avsändares eller mottagares e-postadress.

I underrättelseinhämtning som avser datatrafik görs gränsdragningen mellan styrdata och meddelandets innehållsdata emellertid inte på rent datatekniska grunder. Avgörande för om ett sökbegrepp ska ses som information som beskriver meddelandets innehåll eller som styrdata är teckenföljdens funktion i dataströmmen, det vill säga om sökbegreppets föremål förekommer i den del av dataströmmen som styr innehållet i ett meddelande eller om det är avsett som

ett semantiskt tillägg till meddelandets innehåll som transporteras från avsändaren till mottagaren. Gränsdragningen kan åskådliggöras med fältet ”ämne” i e-postmeddelanden. Detta fält visas i e-postprogram tillsammans med sidhuvudinformationen. Om avsändaren har avsett den som ett budskap till mottagaren av meddelandet, kan den inte ses som styrdata utan ska ses som en del av meddelandets semantiska innehåll som sökbegreppet inte får beskriva. Som sökbegrepp kan däremot e-postadresser, användarnamn för sociala medier och teleadresser användas. Ett sökbegrepp kan också ha en struktur så att det består av en samling styrdata, till exempel en kombination av en IP-adress, en målport och en identifieringsuppgift från transportskiktet. Som sökbegrepp kan även IP-adressområden, autonoma systemnummer (AS-nummer) och domännamn användas. Eftersom till exempel användningen av en viss krypteringsteknik eller ett visst alfabet inte säger något om innehållet i meddelandet, kan även sådana användas som sökbegrepp.

Enligt momentet får sökbegrepp som beskriver det egentliga sakinnehållet i meddelandet trots huvudregeln användas i två fall. Båda undantagen grundar sig på rekommendationer om hur inriktningen av den underrättelseinhämtning som avser datatrafik kan ordnas som den så kallade arbetsgruppen för en informationsanskaffningslag framlagt i sitt betänkande (s. 64 och 80). Enligt dessa rekommendationer är användningen av ett sökbegrepp som beskriver innehållet tillåten bara om det är fråga om datatrafik som inte över huvud taget kan anses omfattas av skyddet för hemligheten i fråga om förtroliga meddelanden. Tyll dessa typer av datatrafik hör främmande staters datatrafik och trafik som innehåller skadeprogram.

Av undantagen sammanhänger det första med främmande stater eller med sådana jämställbara aktörers datatrafik. Enligt den gällande tolkningen omfattas staten och andra offentliga samfund inte av skyddet för de grundläggande fri- och rättigheterna (RP 309/1993 rd och GrUU 9/2015 rd), varför inte heller kommunikation som staten bedriver kan anses omfattas av det grundlagsfästa skyddet för hemligheten i fråga om förtroliga meddelanden. Med en aktör som är jämställbar med en främmande stat avses en aktör som har samma struktur som en myndighet och som inom ett bestämt område utövar självständig och bestående makt. En sådan aktör kan inte heller anses åtnjuta de grundläggande friheterna och rättigheterna.

Om underrättelseinhämtningen kan inriktas uteslutande på en främmande stats eller med en sådan jämställbar aktörs datatrafik, får man enligt bestämmelsen som sökbegrepp använda information som beskriver innehållet i meddelandet. Sökbegreppet kan då bestå av en teckenföljd i meddelandets innehåll, till exempel ett ord eller en mening i ett naturligt språk.

En tillämpning av undantaget som gäller en främmande stats eller med en sådan jämställbar aktörs datatrafik är aktuell bara i de fall där det i den dataström som speglas i underrättelsesystemet inte kan hamna datatrafik som åtnjuter skydd för hemlighet i fråga om förtroliga meddelanden. I praktiken förutsätter detta att den del av kommunikationsnätet som överskrider gränsen och från vilken trafiken speglas till underrättelsesystemet för att jämföras med sökbegrepp har reserverats för statlig datakommunikation.

Det andra undantaget gäller skadliga datorprogram eller datorkommandon. Att ett skadligt datorprogram eller datorkommando är skadligt betyder i bestämmelsen att det äventyrar den tekniska datasäkerheten. Det är alltså fråga om ett program eller kommando som försöker stjäla information från målsystemet, olovligt ändra information i systemet eller försvåra systemets funktion. Som målsystem anses vilket som helst digitalt system, även nätet självt, det vill säga den nätutrustning som styr datatrafiken, samt de anordningar som styr processerna i den reella världen.

De sökbegrepp som beskriver skadliga program och kommandon och som alltså är tillåtna sökbegrepp som beskriver innehållet i meddelanden är i praktiken olika slags tekniska tecken-

följder, inte ord eller uttryck i ett naturligt språk. På grund av sökbegreppens särskilda karaktär ska det inte på motsvarande sätt som i fråga om de sökbegrepp som beskriver innehållet i främmande staters datatrafik krävas att de inte alls ska få tillämpa på datatrafik som faller under skyddet för hemligheten i fråga om förtroliga meddelanden. Det är således tillåtet att jämföra sökbegrepp som beskriver innehållet i skadliga program med en större dataström. Lösningen är såväl tekniskt som till sin innebörd likvärdig med den som det föreskrivs om i 272 § i lagen om tjänster inom elektronisk kommunikation (917/2014) som handlar om åtgärder för informationssäkerheten. Enligt 1 och 2 mom. i paragrafen i fråga har teleföretag, sammanslutningsabonnenter och leverantörer av mervärdestjänster samt aktörer som handlar för dessas räkning rätt att bland annat analysera innehållet i meddelanden automatiskt för att upptäcka och förhindra störningar som kan inverka menligt på informationssäkerheten i kommunikationsnät eller tjänster som anslutits till dem och i informationssystem. Det handlar i praktiken om att ett teleföretag, en sammanslutningsabonnent eller en annan motsvarande aktör som avses i bestämmelsen jämför de igenkänningsdata för skadeprogrammet som används som sökbegrepp med innehållet i alla meddelanden som undersöks.

I 3 mom. anges ett särskilt förbud mot att som sökbegrepp använda uppgifter som specificerar terminalutrustning eller en teleadress som en person, som befinner sig i Finland, innehar eller som denne annars förmodligen använder. Om innehavaren av en terminalutrustning eller en teleadress befinner sig i Finland och skyddspolisen känner till de uppgifter som specificerar utrustningen eller adressen, ska underrättelseinhämtningen utföras med de hemliga metoder för inhämtande av information som anges i det föreslagna 5 a kap. i polislagen, det vill säga teleavlyssning, inhämtande av information i stället för teleavlyssning eller teleövervakning, såvitt villkoren för att använda dessa är uppfyllda. På detta sätt kan konsekvenserna av inhämtningen för utomstående minimeras.

6 § *Fortsatt behandling av information som samlats in med hjälp av automatiserad avskiljning.* I paragrafen föreskrivs det om underrättelsemyndighetens rätt att automatiskt och manuellt behandla information som avskilts från datatrafiken automatiserat på det sätt som avses i 5 §. I motsats till verksamhet enligt 5 § är fortsatt behandling av insamlad information inte sådant tekniskt genomförande av underrättelseinhämtning som avser datatrafik som det föreskrivs om i 10 §. Den ska därför utföras av skyddspolisen, som är civil underrättelsemyndighet, och inte av försvarsmaktens underrättelsetjänst för skyddspolisens räkning.

Med automatisk behandling avses sådan analys av den avskilda informationen som utförs med automatisk databehandling, det vill säga genom ett tekniskt informationssystem. Största delen av analyseringen av insamlade data ska i praktiken genomföras automatiskt. Ett syfte med den automatiska behandlingen är till exempel att utföra sådana sökningar på den insamlade informationen genom vilka den information som ska behandlas manuellt kan reduceras. Den analys och de sökningar som utförs med datorsystemet kan göras på de identifierings- och lokaliseringsdata och övriga styrdata och på det semantiska innehållet i informationen som ingår i den information som samlats in i enlighet med 5 §.

Med manuell behandling avses sensorisk observation som utförs av en fysisk person. Eftersom man vid manuell behandling liksom vid automatisk behandling enligt ovan ska få utreda bland annat innehållet i meddelanden, hör det till den manuella behandlingen till exempel att en tjänsteman vid skyddspolisen utreder textinnehållet i det meddelande som behandlas, granskar bifogade bilder, lyssnar på ljud eller matar in meddelandet i ett program som i laboratorieförhållanden kör sådan exekverbar programkod som ingår i meddelandet som bilaga.

Vid automatisk och manuell behandling får innehållet i meddelanden och andra konfidentiella uppgifter utredas. Med andra konfidentiella uppgifter avses identifieringsuppgifter, förmedlingsuppgifter och lokaliseringsuppgifter. Enligt 5 kap. 8 § 1 mom. i polislagen avses med

identifieringsuppgifter uppgifter om ett meddelande vilka kan förknippas med en abonnent eller användare och behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. I lagen om tjänster inom elektronisk kommunikation har begreppet till skillnad från polislagen ersatts med begreppet förmedlingsuppgifter. Enligt 3 § 40 punkten i lagen om tjänster inom elektronisk kommunikation avses med förmedlingsuppgifter information som kan kopplas till en juridisk eller fysisk person och som behandlas för att överföra meddelanden, samt uppgifter om en radiostations identifieringssignal och radiosändarens användare samt om radiosändningens starttid, varaktighet och utsändningsplats. Begreppet identifieringsuppgifter i polislagen och begreppet förmedlingsuppgifter i lagen om tjänster inom elektronisk kommunikation är alltså inte identiska. I automatisk och manuell behandling enligt den föreslagna paragrafen ska konfidentiella uppgifter likväl få utredas oavsett om de faller under definitionen på identifieringsuppgifter, definitionen på förmedlingsuppgifter eller båda. Med lokaliseringsuppgift avses enligt 3 § 18 punkten i lagen om tjänster inom elektronisk kommunikation information från ett kommunikationsnät eller en terminalutrustning som anger ett abonnemangs eller en terminalutrustnings geografiska position och som används för annat än för att förmedla meddelanden. För ett meddelandes innehåll finns det ingen etablerad definition, men frågan om gränsdragningen mellan meddelandets innehåll och övrig information som omfattas av skyddet för hemligheten i fråga om förtroliga meddelanden har behandlats ovan i samband med motiveringarna till 5 §. Vid tolkningen av denna paragraf har det likväl ingen betydelse hur gränsen dras, eftersom den utredningsrätt som anges i paragrafen så som ovan konstaterats gäller alla uppgifter som omfattas av hemligheten i fråga om förtroliga meddelanden. Vid sidan av de uppgifter enligt ovan som omfattas av skyddet för hemligheten i fråga om förtroliga meddelanden ska det enligt förslaget utan särskilt omnämnande på författningsnivå vara tillåtet att utreda också sådana data med anknytning till styrningen av datatrafiken som inte omfattas av hemligheten i fråga om förtroliga meddelanden

Den rätt att utreda innehållet i ett meddelande som avses i paragrafen inbegriper också rätten att utreda innehållet i datatrafik i samband med att information som sparas genom molntjänster, till exempel innehållet i ett dokument som ska sparas i eller hämtas från en molntjänst.

Om det under automatisk eller manuell fortsatt behandling visar sig att den uppgift som är föremål för behandlingen omfattas av förbudet mot underrättelseinhämtning i 12 § eller om uppgiften inte behövs för värnandet av den nationella säkerheten, ska den enligt 15 § utplånas utan dröjsmål.

7 § *Domstolens tillstånd för underrättelseinhämtning som avser datatrafik.* I paragrafen föreskrivs det om domstolens tillstånd för underrättelseinhämtning som avser datatrafik och om yrkande och beslut om underrättelseinhämtning som avser datatrafik.

Enligt 1 mom. ska domstolen besluta om underrättelseinhämtning som avser datatrafik på skriftligt yrkande av chefen för skyddspolisen. Med avvikelse från de hemliga metoder för inhämtande av information som det föreskrivs om i 5 kap. i polislagen krävs det uttryckligen att yrkandet om användning av metoden ska ha skriftlig form. Det skriftliga yrkandet kan bara lämnas av skyddspolisens chef, vilket även det är en avvikande lösning i jämförelse med de hemliga metoder för inhämtande av information som regleras i 5 kap. i polislagen. Att det krävs en så hög tjänsteställning av den yrkande kan motiveras med att underrättelseinhämtning som avser datatrafik till sin karaktär avviker från övriga metoder för informations- och underrättelseinhämtning. Trots att det är skyddspolisens chef som ska lämna ansökan, ska det inte av detta följa att denne måste närvara personligen när domstolen behandlar yrkandet. Vid behandlingen kan skyddspolisen i stället för chefen företrädas av en annan tjänsteman som utsetts av chefen och som har satt sig in i det ärende som yrkandet gäller.

I 2 mom. föreskrivs det om de omständigheter som ska nämnas i skyddspolisens chefs yrkande till domstolen och i domstolens beslut med anledning av detta.

Enligt 1 punkten i momentet ska det i yrkandet och i beslutet nämnas den i 3 § avsedda verksamhet som allvarligt hotar den nationella säkerheten och som är föremål för underrättelseinhämtningen. Av yrkandet och beslutet ska det följaktligen framgå av vilken verksamhet eller vilka verksamheter enligt den nämnda paragrafen som det är meningen att information ska inhämtas genom underrättelseinhämtning som avser datatrafik.

Enligt 2 punkten i momentet ska det i yrkandet och beslutet anges fakta om den verksamhet som allvarligt hotar den nationella säkerheten. Det krävs att skyddspolisen i sitt yrkande för domstolen tillräckligt utförligt redogör för karaktären av den konkreta verksamhet om vilken information ska inhämtas genom underrättelseinhämtningen. De uppgifter som ges i yrkandet kan röra till exempel hur skyddspolisen fått kännedom om verksamheten, hur verksamheten dittills har tagit sig uttryck, hur det antas att verksamheten utvecklas och vilken aktör eller vilka personer som står bakom verksamheten. Skyddspolisen ska på ett sätt som övertygar domstolen påvisa att den verksamhet som är föremål för yrkandet på grundval av kända konkreta fakta motsvarar den typ av hot som avses i 3 § och som det hänvisas till i föregående punkt.

Enligt 3 punkten ska det i yrkandet och i beslutet anges vilka fakta förutsättningarna för underrättelseinhämtning som avser datatrafik grundar sig på. I yrkandet och i beslutet ska det för det första motiveras varför kravet i 4 § 1 mom. om att underrättelseinhämtning som avser datatrafik ska vara resultatrik är uppfyllt. Skyddspolisen ska i sitt yrkande redogöra för de omständigheter på grundval av vilka den genom underrättelseinhämtning som avser datatrafik kan antas få uppgifter om den verksamhet som yrkandet gäller och som allvarligt hotar den nationella säkerheten. Om yrkandet inte gäller enbart underrättelseinhämtning som riktar sig mot en främmande stats eller med en sådan jämställbar aktörs datatrafik, ska skyddspolisen i yrkandet dessutom redogöra för hur nödvändighetsvillkoret i 4 § 2 mom. uppfylls. I yrkandet och likaså i domstolens beslut ska det redogöras för varför de uppgifter som ska inhämtas genom underrättelseinhämtningen inte kan inhämtas på annat sätt eller varför inhämtning på annat sätt är väsentligt svårare.

Enligt 4 punkten ska det i yrkandet och i beslutet anges vilka sökbegrepp eller kategorier för sökbegrepp som ska användas i den underrättelseinhämtning som avser datatrafik samt motiveringarna till dem. Sökbegrepp som kan användas vid underrättelseinhämtning som avser datatrafik och exempel på sådana har behandlats ovan i detaljmotiveringarna till 5 §. Utöver sökbegrepp kan yrkandet som framläggs för domstolen också gälla sökbegreppens kategori. Med denna hänvisar man inte - till skillnad från vad som är fallet med sökbegrepp - till en enskild teknisk uppgift som utan bearbetning kan användas som jämförelsevillkor vid automatiserad avskiljning utförd på datatrafik. Med kategori av sökbegrepp avses en exakt avgränsad verbal beskrivning av sökbegrepp som är relevanta med hänsyn till den fråga som underrättelseinhämtningen gäller. Tillstånd för användning av en kategori av sökbegrepp ska enligt förslaget kunna sökas hos domstolen när det till samma helhet som kan avgränsas tillräckligt exakt hör en mängd sökbegrepp av samma typ av vilka bara en del är kända när underrättelseinhämtningen som avser datatrafik inleds. I stället för att det på grundval av ny information som fås genom underrättelseinhämtningen alltid inleda ett nytt tillståndsförfarande för att sökbegreppen ska godkännas, ska domstolens tillstånd enligt förslaget kunna gälla en verbal beskrivning av en kategori av sökbegrepp, varvid de enskilda sökbegrepp som skapas utifrån den nya informationen omfattas av det tillstånd som sökts tidigare.

I 5 § i den svenska signalspaningslagen och i 40 § i den schweiziska spaningslagen föreskrivs det om godkännande av kategorier av sökbegrepp som grund för underrättelseinhämtning som avser datatrafik på motsvarande sätt som i detta förslag.

En kategori av sökbegrepp kan till exempel utgöras av en beskrivning av kontakterna för en grupp av personer som specificeras i skyddspolisens yrkande. Faktorer som förenar personerna i gruppen kan till exempel vara att de är medlemmar i en viss terroristgrupp eller sköter en viss arbetsuppgift i en sådan organisation som representerar en främmande stat och vars verksamhet allvarligt hotar Finlands nationella säkerhet. Om man genom underrättelseinhämtningen får reda på teleadressrymderna för personer som hör till gruppen samt andra utländska teleadresser, kan de användas som sökvillkor. För att kontakterna för en grupp av personer ska kunna godkännas som en kategori av sökbegrepp krävs att grunderna för medlemskap i gruppen angetts tillräckligt exakt i yrkandet, att det visats att gruppen utgör ett allvarligt hot mot den nationella säkerheten och att yrkandet även i övrigt uppfyller förutsättningarna för underrättelseinhämtning som avser datatrafik.

Som kategori av sökbegrepp kan även dataförbindelserna mellan Finland och ett tillräckligt litet geografiskt område som specificeras i ansökan och godkännas. Det geografiska området kan till exempel vara en viss terroristgrupps kommandoplats från vilken man vet att gruppen styr medlemmar i Finland. För att de kontakter som hänför sig till ett visst geografiskt område ska kunna godkännas som kategori av sökbegrepp, måste underrättelsemyndigheten kunna påvisa områdets betydelse för en verksamhet som allvarligt hotar den nationella säkerheten. Den ska också vid behov specificera de gränser inom vilka konkreta sökvillkor utformas för att underrättelseinhämtningen inte ska rikta sig mot datatrafik som i trots att den har sitt ursprung i det geografiska området i fråga är ovidkommande med hänsyn till hotet.

Som kategorier av sökbegrepp kan även skadliga program som en bestämd underrättelsetjänst i en främmande stat använder i sitt cyberspionage eller nätadresser som underrättelsetjänsten i fråga använder som verktyg i sitt cyberspionage komma på fråga. Om den skadliga programkoden eller nätadresserna specificeras i yrkandet är det fråga om sökbegrepp och inte kategorier av sökbegrepp. Behovet att ansöka om tillstånd för kategorier av sökbegrepp som består av skadlig programkod och nätadresser som används för cyberspionage beror på att koden och adresserna kan ändras medan underrättelseinhämtningen pågår och på att underrättelseinhämtningens kan leda till ny kunskap om dem. En underrättelsetjänst som använder ett skadeprogram i sitt cyberspionage kan till exempel modifiera programkoden så att den inte längre motsvarar den ursprungliga, varvid ett enskilt sökbegrepp som domstolen har beviljat tillstånd att använda inte längre kan identifiera koden. Om skyddspolisen kan begära och få ett generellt tillstånd för de skadeprogram som underrättelsetjänsten använder (kategori av sökbegrepp), kan underrättelseinhämtningen utan avbrott riktas mot den modifierade koden.

Om tillstånd för underrättelseinhämtning som avser datatrafik kunde begäras bara för enskilda nätadresser (sökbegrepp) som används som verktyg vid cyberspionage skulle man på motsvarande sätt vara tvungen att avbryta underrättelseinhämtningen om aktören som bedriver spionage styr om trafiken. En oavbruten underrättelseinhämtning som avser datatrafik förutsätter att tillstånd begärts och beviljats generellt för de adresser (den kategori av sökbegrepp) som den underrättelsetjänst som nämns i yrkandet använder som verktyg.

De uppgifter som kommer på fråga som tillåtna kategorier av sökbegrepp är omöjliga att fastställa på förhand på ett uttömmande sätt. Följaktligen föreslås det att domstolspraxis ska få klargöra hurdan en grupp av inbördes relaterade data ska vara för att anses tillräckligt precis för att kunna utgöra en kategori av sökbegrepp. När domstolen godkänner en viss kategori av sökbegrepp, får den ange sådana begränsningar och närmare villkor för användningen som föreslås senare i punkt 9 i momentet.

När domstolen godkänner en kategori av sökbegrepp ges underrättelsemyndigheten begränsad rätt att själv utforma de konkreta sökbegrepp som används vid underrättelseinhämtningen, varför det finns behov att göra denna verksamhet till föremål för noggrann övervakning. Övervakningen gäller frågan om valet av konkreta sökbegrepp sker inom ramen för den kategori som domstolen godkänt i sitt beslut. Bestämmelser om övervakningen föreslås ingå i lagen om övervakning av underrättelseverksamheten (/).

I yrkandet och i beslutet anges även grunderna för de sökbegrepp eller kategorier av sökbegrepp som ska användas i underrättelseinhämtning som avser datatrafik. Som framgår av motiveringarna till 4 § är sökbegreppen i regel tekniska uppgifter vars samband med en verksamhet som är föremål för underrättelseinhämtningen och som allvarligt hotar den nationella säkerheten inte nödvändigtvis förefaller sig uppenbar. Den som framlägger yrkandet ska därför för domstolen redogöra för hur sökbegreppet sammanhänger med en verksamhet som allvarligt hotar den nationella säkerheten och varför man genom användning av sökbegreppet antas få information om verksamheten i fråga samt vilken information man genom användningen av sökbegreppet sannolikt får. Om sökbegreppet till exempel är en IP-adressrymd, ska underrättelsemyndigheten klargöra på vilka grunder datatrafik som sammanhänger med en verksamhet som allvarligt hotar den nationella säkerheten antas försiggå i adressrymden i fråga och av vilket slag trafiken är. Om yrkandet gäller en kategori av sökbegrepp ska underrättelsemyndigheten redogöra för sambandet mellan den valda kategorin av sökbegrepp och en verksamhet som ska utredas genom underrättelseinhämtningen och som allvarligt hotar den nationella säkerheten, hur de tekniska sökbegreppen ska bildas inom ramen för kategorin och vilket slags information som ska inhämtas med hjälp av sökbegreppen.

Enligt 5 punkten ska det i yrkandet och i beslutet anges i vilken del av kommunikationsnätet sökbegreppen ska används på den datatrafik som rör sig där samt motiveringar till att denna del av kommunikationsnätet väljs. Sökbegrepp får inte användas på all trafik som överskrider gränsen, utan användningen av dem ska begränsas till den del av datatrafiken som det är nödvändigt att granska i det aktuella fallet. Till den civila underrättelsemyndighetens skyldigheter hör att i sitt yrkande om tillstånd så exakt som möjligt specificera den del av kommunikationsnätet i vilken datatrafiken jämförs med sökbegreppen. De uppgifter om vilken del av nätet det är fråga om som fordras i yrkandet och i beslutet ska enligt förslaget utredas antingen genom den fullmakt att behandla de tekniska data som föreslås i 66 § i lagen om militär underrättelseverksamhet eller genom dataöverförarens skyldighet att lämna information enligt 22 § i den aktuella lagen. När delen av kommunikationsnätet utreds, kommer en kombination av de utredningsmetoder som nämns ovan oftast att användas.

Den behandling av tekniska data i kommunikationen som anges i den föreslagna 66 § i lagen om militär underrättelseverksamhet är i första hand avsedd att vara en metod för att utreda hur relativt statiska strömmar i datatrafiken dirigeras i ett nät som överskrider landsgränsen. För att göra det möjligt att även i den civila underrättelseinhämtningen utnyttja verksamhet enligt bestämmelsen i fråga, ska 10 § 2 mom. i lagen om civil underrättelseinhämtning avseende datatrafik innehålla en bestämmelse enligt vilken skyddspolisen får ge försvarsmaktens underrättelsetjänst i uppdrag att behandla tekniska data. Försvarsmaktens underrättelsetjänst ska då söka tillstånd att behandla tekniska data vid kommunikation enligt 67 § i lagen om militär underrättelseverksamhet hos domstolen även för skyddspolisens räkning.

De uppgifter som fås inom ramen för den informationsskyldighet som det enligt förslaget ska föreskrivas om i 22 § är nödvändiga särskilt när man utreder i vilken del av ett kommunikationsnät annan än statiskt dirigerad datatrafik kan antas överskrida Finlands gräns. Genom paragrafen åläggs dataöverföraren att på en specificerad begäran av skyddspolisen ge sådan information som den innehar och som är nödvändig för att specificera en del av kommunikationsnätet för tillståndsyrkandet och tillståndsbeslutet. Eftersom dataöverförarnas uppgifter om

hurdan datatrafik som förekommer i de datanät som de äger eller innehar och som överskrider gränserna är rätt summariska, kan det i visa fall hända att man i tillståndsvillkoren bara kan utesluta sådana delar av ett kommunikationsnät där man kan anta att det inte förekommer datakommunikation som sammanhänger med verksamhet som allvarligt hotar den nationella säkerheten. Yrkandet kan därför även gälla en rätt stor del av ett kommunikationsnät

Trots de särskilda användningsområdena för de två metoder som nämns ovan kommer man vid utredningen av den aktuella delen av kommunikationsnätet i praktiken oftast att använda en kombination av dem. När man utreder hur den statiska datatrafiken dirigeras över gränsen är uppgifter från dataöverförarna i inledningsskedet nödvändiga för att den befogenhet som avses i 66 § i lagen om militär underrättelseverksamhet ska kunna användas så välriktat och rationellt som möjligt. När dirigeringen av annan datatrafik än den statiskt dirigerade utreds ska de uppgifter som fåtts från dataöverförarna kunna verifieras genom verksamhet som avses i 66 § i lagen om militär underrättelseverksamhet. Dessutom kan denna verksamhet ge upphov till sådan ny uteslutande information som dataöverföraren inte innehade. Användningen av exkluderande information gör det möjligt att sökbegrepp för underrättelseinhämtning som avser datatrafik inte används på datatrafiken i en större del av det kommunikationsnät som överskrider gränsen.

I yrkandet och i beslutet ska motiveringar till valet av den del av nätet där sökbegrepp ska användas på datatrafiken ingå. Det förutsätts alltså att den civila underrättelsemyndigheten i sitt yrkande redogör för varför och på vilka grunder datatrafik som har samband med verksamhet som allvarligt hotar den nationella säkerheten kan antas ske i den del av datanätet som yrkandet gäller.

Enligt 6 punkten ska giltighetstiden för tillståndet till underrättelseinhämtning som avser datatrafik anges i yrkandet och i beslutet med angivande av klockslag. Punkten motiveras på samma sätt som 5 a kap. 6 § 4 punkten i polislagen.

Enligt 7 punkten ska den polisman som hör till skyddspolisens befäl och är förordnad att leda och övervaka underrättelseinhämtningen och som är förtrogen med användningen av metoder för underrättelseinhämtning anges i yrkandet och i beslutet. För motiveringar till punkten hänvisas till motiveringarna till 5 a kap. 6 § 5 punkten i polislagen.

Enligt 8 punkten ska eventuella begränsningar i och villkor för den underrättelseinhämtning som avser datatrafik anges i yrkandet och i beslutet. Om det finns kännedom om sådana begränsningar och villkor redan när yrkandet utarbetas, finns det skäl att ange dem där. Begränsningar och villkor ska kunna anges till exempel för hur underrättelsemyndigheten ska få bilda sökbegrepp inom ramen för de kategorier av sökbegrepp som domstolen beviljar tillstånd för.

I 3 mom. ska det enligt förslaget föreskrivas om den maximala giltighetstiden för ett tillstånd som gäller underrättelseinhämtning som avser datatrafik. Den längsta giltighetstiden för ett tillstånd som gäller underrättelseinhämtning som avser datatrafik är enligt momentet sex månader. I 5 § i den svenska signalspaningslagen och i 40 § i den schweiziska spaningslagen anges motsvarande längsta giltighetstider. Den längsta giltighetstiden för ett tillstånd som gäller underrättelseinhämtning som avser datatrafik är dessutom enligt förslaget lika lång som den längsta giltighetstiden för tillstånd och beslut enligt 5 a kap. i polislagen. Den tillståndstid på sex månader som föreslås innebär inte automatiskt att tillstånd alltid kan sökas för sex månader eller att de ska beviljas för sex månader. I själva verket förutsätter uttrycket ”för högst sex månader åt gången” i bestämmelsen en bedömning enligt proportionalitetsprincipen och principen om minsta olägenhet. När tillstånd söks och beviljas ska man därför bedöma hur länge underrättelseinhämtning som avser datatrafik behöver användas från fall till fall.

Enligt 4 mom. ska underrättelseinhämtning som avser datatrafik avslutas före utgången av den tidsfrist som anges i beslutet, om syftet med underrättelseinhämtningen som avser datatrafik har nåtts eller om det inte längre finns förutsättningar för det. Genom bestämmelsen betonas att underrättelseinhämtning under inga omständigheter får användas under längre tid än nödvändigt även om domstolens tillstånd fortfarande är i kraft.

8 §. *Förfarandet i domstol.* Enligt paragrafen iakttas vid handläggning och avgörande i domstol av tillståndsärenden som gäller underrättelseinhämtning som avser datatrafik vad som föreskrivs i 5 a kap. 35 § i polislagen om behandlingen av tillståndsärenden som gäller metoder för underrättelseinhämtning.

För motiveringen till paragrafen hänvisas till motiveringen till den aktuella paragrafen i 5 a kap. i polislagen.

9 §. *Beslutsförfarande i brådskande situationer.* I paragrafen föreskrivs det om beslutsförfarandet i brådskande situationer som gäller underrättelseinhämtning som avser datatrafik där det är chefen för skyddspolisen som beslutar om att underrättelseinhämtningen ska inledas. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att underrättelseinhämtningen inleddes. Om domstolen anser att de förutsättningar för underrättelseinhämtning som avser datatrafik som anges i 4 § inte är uppfyllda, ska underrättelseinhämtningen avslutas omedelbart.

Paragrafen har utformats med 5 kap 10 § 2 mom. och 12 § 1 mom. i polislagen och 10 kap. 9 § 1 mom. och 11 § 1 mom. i tvångsmedelslagen som huvudsakliga modeller. Enligt dessa får en anhållningsberättigad tjänsteman i brådskande fall besluta om teleövervakning och inhämtande av basstationsuppgifter till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. När det gäller underrättelseinhämtning som avser datatrafik föreskrivs det om ett liknande beslutsförfarande i brådskande situationer i 5 b § i den svenska signalspaningslagen. Med avvikelse från de bestämmelser i polislagen och i tvångsmedelslagen som nämns ovan föreslås det att befogenheten att fatta ett tillfälligt brådskande beslut i skyddspolisens organisation ska tillhöra skyddspolisens chef ensam.

På det sätt som framgår av den allmänna motiveringen har Europadomstolen i sin avgörandepraxis ansett att de särskilda bestämmelserna om beslutsförfarandet i brådskande situationer kan vara godtagbara om det av den nationella lagen klart framgår att ett sådant beslutsförfarande kan tillämpas bara i undantagsfall och när nödvändiga orsaker föreligger. Liksom de ovan nämnda bestämmelserna i polislagen, tvångsmedelslagen och den svenska signalspaningslagen föreslås det att en förutsättning för användning av förfarandet för brådskande fall ska vara att ärendet som gäller underrättelseinhämtning som avser datatrafik inte bör fördröjas. Behovet att använda underrättelseinhämtning som avser datatrafik kan ibland uppstå så snabbt att den fördröjning som skulle bli följden av tillståndssökande enligt det förfarande som anges i 7 § allvarligt skulle hota den nationella säkerheten. Det kan till exempel vara fråga om ett omedelbart och allvarligt hot med anknytning till internationell terrorism. Förutsättningen för användningen av förfarandet uppfylls också i situationer där det i och för sig inte finns ett hot men där den fördröjning som sökande av tillstånd medför skulle leda till att det material som skulle kunna fås genom underrättelseinhämtningen går oåterkalleligt förlorat. På grund av att underrättelseinhämtning som avser datatrafik består av flera faser bedöms det att förutsättningarna för att förfarandet för brådskande situationer kommer att uppfyllas klart mera sällan än när det gäller till exempel teleövervakning. Utformningen av de sökbegrepp som används vid automatisk avskiljning är till exempel en så pass tidskrävande process att det i allmänhet är möjligt att söka tillstånd för underrättelseinhämtning som avser datatrafik hos domstolen innan ett brådskande beslut som innehåller sökbegreppen är färdigt att lämnas till den myndighet som svarar för det tekniska genomförandet.

Ett brådskande beslut om underrättelseinhämtning som avser datatrafik ska utfärdas skriftligt. Genom detta krav ska det säkerställas att domstolen när den senare behandlar ärendet kan konstatera om de krav som ställs på underrättelseinhämtning som avser datatrafik var uppfyllda vid den tidpunkt då det brådskande beslutet fattades. Genom kravet att det brådskande beslutet ska ha skriftlig form garanteras också att beslutet och omständigheterna när det fattades kan utsättas för tillräckligt effektiv laglighetskontroll i efterhand. Kravet på skriftlig form ska gälla samtliga nio punkter i 7 § 2 mom.

Ett ärende som gäller underrättelseinhämtning som avser datatrafik ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att underrättelseinhämtningen inleddes. Ärendet ska föras till domstol även i de fall där underrättelseinhämtningen avslutas inom 24 timmar efter att den inleddes. Annars skulle man med mycket kortvarigt inhämtande av information kunna kringgå de krav som enligt förslaget ska ställas på beslutsförfarandet och den skyldighet att utplåna uppgifter som ingår i det föreslagna 2 mom.

I 2 mom. föreskrivs det om följderna av domstolens avgörande i det fall att domstolen anser att förutsättningar för underrättelseinhämtning för vilken tillstånd beviljats genom ett förfarande enligt 1 mom. helt eller delvis saknades.

Enligt första meningen i momentet ska underrättelseinhämtningen avslutas omedelbart och det material som inhämtats genom underrättelseinhämtningen och anteckningarna om de uppgifter som inhämtats genom den genast utplånas, om domstolen anser att det inte funnits förutsättningar enligt 4 § för underrättelseinhämtning som avser datatrafik. I paragrafen som det hänvisas till ingår bestämmelser om krav som gäller resultat och nödvändighet. Om domstolen anser att beslutet som fattats genom förfarandet för brådskande situationer inte har uppfyllt förutsättningarna för underrättelseinhämtning som avser datatrafik, kan beslutet anses vara så fundamentalt felaktigt att användningen av underrättelseinhämtning helt och hållet ska avslutas och det material som inhämtats genom den och de anteckningar som gjorts utplånas i sin helhet.

I andra meningen i momentet föreskrivs det om de situationer där domstolen av någon annan anledning än avsaknaden av de förutsättningar som avses i 4 § anser att det brådskande beslutet varit felaktigt. Ett sådant annat fel kan i vissa situationer vara så allvarligt att det kan jämställas med avsaknaden av de förutsättningar som avses i 4 §, medan det i andra situationer är så lindrigt eller partiellt att det kan anses oskäligt att helt avsluta underrättelseinhämtningen. I den föreslagna lagstiftningen har man strävat efter att beakta att förfarandet med brådskande beslut i praktiken blir aktuella i särskilt allvarliga situationer för att få uppgifter om faror som omedelbart hotar, och att det i beslut som fattas i sådana situationer kan förekomma smärre fel.

Om ett brådskande beslut som gäller användningen av underrättelseinhämtning som avser datatrafik är gravt felaktigt till exempel därför att den verksamhet som varit föremål för underrättelseinhämtningen inte motsvarar någon av de verksamheter som anges i den föreslagna 3 § eller om de konkreta fakta som man känner till om verksamheten är otillräckliga som grund för ett beslut om underrättelseinhämtningen, ska felets allvarlighet jämställas med avsaknaden av de förutsättningar för underrättelseinhämtning som anges i 4 §. I så fall ska underrättelseinhämtningen avslutas helt och hållet i enlighet med domstolens beslut, och det material som inhämtats genom den och de anteckningar som gjorts utplånas i sin helhet. Som partiellt fel kan man till exempel anse det att något eller några av de sökbegrepp som nämns i det brådskande beslutet inte har varit tillräckligt exakta eller i tillräcklig grad svarat mot den hotande verksamhet som är föremål för informationsinhämtningen medan övriga sökbegrepp varit oklanderliga. Om domstolen avgör ärendet på detta sätt, ska användningen av de felaktiga sökbegreppen avslutas omedelbart och det material som inhämtats och de anteckningar som gjorts

på grundval av användningen utan dröjsmål utplånas. I övrigt ska underrättelseinhämtningen kunna fortsätta i den utsträckning som domstolen tillåter, och de uppgifter som fås tack vare detta sparas. En situation som gäller partiell avslutning av underrättelseinhämtningen och utplåning av den information som inhämtats genom de delar av inhämtningen som avslutas kan uppstå även när de delar av ett kommunikationsnät som nämns i ett brådskande beslut om underrättelseinhämtning och där inhämtningen genomförs till vissa delar har specificerats rätt och till vissa delar fel.

Enligt tredje meningen i momentet ska en uppgift som inhämtats med stöd av ett brådskande beslut som upphävts av domstolen dock få bevaras och lagras i ett register som uppfyller kraven i lagen om behandling av personuppgifter i polisens verksamhet i enlighet med de förutsättningar som anges i 5 a kap. 45 § 1 mom. i polislagen. Uppgiften ska enligt den bestämmelsen utplånas utan dröjsmål efter att det framgått att den inte behövs för dessa syften. I 5 a kap. 45 § 2 mom. i polislagen finns det även en hänvisning till 5 a kap. 46 § i polislagen, som rör utplåningen av uppgifter som inhämtats i brådskande situationer med de metoder för underrättelseinhämtning som avses i kapitlet. Förutsättningarna för att använda uppgifter som inhämtats genom brådskande beslut som konstaterats vara felaktigt blir då de samma när informationen inhämtats genom underrättelseinhämtning som avser datatrafik som när den inhämtats genom de metoder för underrättelseinhämtning som avses i 5 a kap. i polislagen.

10 §. *Tekniskt genomförande av underrättelseinhämtning som avser datatrafik och annat samarbete med militärunderrättelsemyndigheten.* I paragrafen föreskrivs det om det tekniska genomförandet av underrättelseinhämtning som avser datatrafik. Det tekniska genomförandet av underrättelseinhämtning som avser datatrafik sköts av försvarsmaktens underrättelsetjänst på uppdrag av skyddspolisen. Det tekniska genomförandet omfattar dels de åtgärder som avses i 63 § i lagen om militär underrättelseverksamhet, för vilka försvarsmaktens underrättelsetjänst ska ansöka om tillstånd för skyddspolisens räkning, dels åtgärderna enligt 5 § i denna lag, för vilka av skyddspolisen söker tillstånd hos domstolen eller som skyddspolisens chef i exceptionella brådskande situationer kan fatta tillfälliga beslut om. Till det tekniska genomförandet hör enligt förslaget också att försvarsmaktens underrättelsetjänst lämnar uppdragsgivaren skyddspolisen den information som den inhämtat inom ramen för sitt uppdrag.

Enligt 1 mom. är försvarsmaktens underrättelsetjänst teknisk utförare av den underrättelseinhämtning som avser datatrafik. Att försvarsmaktens underrättelsetjänst utses till teknisk utförare grundar sig på ett förslag av arbetsgruppen för en informationsanskaffningslag. Enligt vad arbetsgruppens framlagt i sitt slutbetänkande är det inte ändamålsenligt om de myndigheter som behöver underrättelseinformation var för sig bedriver underrättelseinhämtning som avser datatrafik, utan kraven på att verksamheten är enhetlig och kan hållas hemlig, den specialisering och det tekniska kunnande som den förutsätter samt synpunkter som sammanhänger med övervakningen av verksamhetens laglighet motiverar att en myndighet sköter det tekniska genomförandet av underrättelseinhämtningen för samtliga myndigheters räkning.

I 2 mom. föreskrivs det om det uppdragsförfarande som tillämpas vid behandlingen av tekniska data. Behandlingen av tekniska data är metod med vilken man för det tillståndsyrkande för underrättelseinhämtning som avser datatrafik som senare ska lämnas in hos domstolen kan utreda i vilken del av kommunikationsnätet sökbegrepp behöver användas på datatrafiken. Bestämmelser om behandlingen av tekniska data finns i 63 § i den föreslagna lagen om militär underrättelseverksamhet och bestämmelser om tillståndsförfarandet för behandlingen i 64 § i samma lag. Enligt 1 mom. i den förra paragrafen ska försvarsmaktens underrättelseinhämtning ha rätt att i datatrafiken i ett kommunikationsnät kortvarigt samla in och lagra tekniska data om datatrafiken och med hjälp av automatisk databehandling behandla dem för statistisk analys. I denna statistiska analys utreds i vilken del av kommunikationsnätet datatrafik som har samband med hotande verksamhet sannolikast förekommer. Enligt 64 § i lagen om militär

underrättelseverksamhet beslutar en domstol om behandlingen av tekniska data på yrkande av en tjänsteman som getts särskild utbildning i användningen av underrättelseinhämtningsmetoderna. I paragrafen föreskrivs det också om vilka uppgifter som ska framgå av det yrkande som framläggs för domstolen och av domstolens beslut.

Genom uppdragsförfarandet blir det möjligt att utnyttja den befogenhet enligt lagen om militär underrättelseverksamhet som behövs för att utreda en del av ett kommunikationsnät i den civila underrättelseinhämtningen. Enligt bestämmelsen ska skyddspolisen kunna ge försvarsmaktens underrättelsetjänst i uppdrag att behandla tekniska data, varefter underrättelsetjänsten ansöker om tillstånd för åtgärden i fråga hos domstolen. Efter att ha fått tillstånd av domstolen och efter att ha genomfört de åtgärder tillståndet gäller ska försvarsmaktens underrättelsetjänst lämna skyddspolisen resultatet av sin statistiska analys.

I samband med att skyddspolisen ger försvarsmaktens underrättelsetjänst i uppdrag att behandla tekniska data ska den lämna underrättelsetjänsten uppgifter som är nödvändiga för att uppdraget ska kunna genomföras så väl inriktat och så rationellt som möjligt. Till dessa uppgifter hör bland annat en preliminär beskrivning av de sökbegrepp som ska användas senare i underrättelseinhämtningen samt uppgifter om det geografiska område från vilket den datatrafik som sammanhänger med den verksamhet som ska utredas genom underrättelseinhämtningen härrör. Dessutom ska skyddspolisen lämna försvarsmaktens underrättelsetjänst sådana uppgifter som är väsentliga för ärendet och som den har fått av dataöverföraren eller dataöverförarna med stöd av deras informationsskyldighet enligt den föreslagna 22 §. Dessa uppgifter från dataöverförare har en exkluderande betydelse, eftersom den momentana provtagning som ingår i behandlingen av tekniska data med hjälp av dem kan begränsas till den del av kommunikationsnätet där den datatrafik som är väsentlig med hänsyn till underrättelseinhämtningen kan röra sig. Enligt 64 § 3 mom. i lagen om militär underrättelseverksamhet ska det av det tillståndsyrkande rörande behandlingen av tekniska data som framläggs för domstolen framgå i vilka delar av kommunikationsnätet tekniska data kortvarigt ska samlas in.

Det tillstånd för behandling av tekniska data som avses i 64 § i lagen om militär underrättelseverksamhet ska för skyddspolisens del sökas av försvarsmaktens underrättelsetjänst. Orsaken till att detta förfarande föreslås är att det av tillståndsyrkandet enligt 3 mom. ska framgå vissa uppgifter som anknyter till behandlingen och organiseringen av teknisk information om vilka försvarsmaktens underrättelsetjänst besitter den bästa kunskapen. Till dessa uppgifter hör uppgifter om den tjänsteman inom den militära underrättelseinhämtningen som leder verksamheten samt en plan för hur den verksamhet som yrkandet gäller ska genomföras av den militära underrättelsemyndigheten.

Efter att ha genomfört behandlingen av tekniska data för skyddspolisens räkning, ska försvarsmaktens underrättelsetjänst lämna skyddspolisen resultatet av den statistisk analys som den utarbetat inom ramen för behandlingen. Resultatet av den statistiska analysen visar för vilken del av kommunikationsnätet skyddspolisen i följande skede bör ansöka om tillstånd för underrättelseinhämtning som avser datatrafik enligt 7 § i lagen om civil underrättelseinhämtning avseende datatrafik.

Enligt första meningen i 3 mom. ska skyddspolisen lämna det beslut om användning av underrättelseinhämtning som avser datatrafik som avses i 7 eller 9 § till försvarsmaktens underrättelsetjänst som utför de uppgifter som avses i 5 § för skyddspolisens del. I den 5 § som det hänvisas till föreslås bestämmelser om hur underrättelseinhämtning som avser datatrafik ska inriktas, vilket är en uppgift av teknisk karaktär som således ska utföras av försvarsmaktens underrättelsetjänst. I praktiken genomförs inriktningen så att försvarsmaktens underrättelsetjänst i det tekniska system som används vid underrättelseinhämtningen matar in de sökbegrepp som godkänts genom domstolens tillståndsbeslut eller skyddspolisens chefs brådskande

beslut. De konkreta sökbegreppen framgår likväl inte alltid av beslutet, eftersom det enligt den föreslagna 7 § 3 mom. 4 punkt vid sidan av eller i stället för sökbegrepp går att få godkännande även för kategorier av sökbegrepp. Det tekniska genomförandet av underrättelseinhämtningen ska inte medföra rätt att utveckla och precisera sökbegreppen inom ramen för de kategorier av sökbegrepp som godkänts i beslutet, utan konkretiseringen av sökbegreppen ska vara enbart uppdragsgivarens, det vill säga skyddspolisens, uppgift. Den tekniska utföraren ansvarar därför inte heller rättsligt för att sökbegreppen har bildats rätt utan endast för att de har matats in i det tekniska systemet för filtrering av datatrafiken i enlighet med uppdraget.

Vid den automatiserade filtrering som utförs av försvarsmaktens underrättelsetjänst avskiljs den del av datatrafiken som motsvarar sökbegreppen och som à priori är av betydelse med hänsyn till det hot som utreds. Försvarsmaktens underrättelsetjänst tar hand om denna del av datatrafiken för att överlämna den till skyddspolisen. Försvarsmaktens underrättelsetjänst har inte inom ramen för det tekniska genomförandet rätt att behandla den datatrafik som den tagit hand om automatiskt eller manuellt på det sätt som anges i den föreslagna 6 §, utan rätt till fortsatt behandling av den datatrafik som tagits om hand ska endast uppdragsgivaren ha. Det tekniska genomförandets rent tekniska natur ger för sin del även det föreslagna 73 § 3 mom. i lagen om militär underrättelseverksamhet uttryck för. Enligt det momentet får försvarsmaktens underrättelsetjänst inte utreda ett meddelandes innehåll i samband med det tekniska genomförandet av underrättelseinhämtning som avser datatrafik.

Enligt den andra meningen i momentet ska försvarsmaktens underrättelsetjänst lämna de data som den samlat för att genomföra uppdraget till uppdragsgivaren, det vill säga till skyddspolisen. När försvarsmaktens underrättelsetjänst tar hand om data om via det tekniska genomförandet av underrättelseinhämtningen som avser datatrafik är det en tillfällig åtgärd vars syfte endast är att göra det möjligt att överlämna dem till den myndighet som svarar för behandlingen. Försvarsmaktens underrättelsetjänst ska inte ha rätt att lagra dessa data annat än tillfälligt, utan de ska alltså försvinna ur dess system i och med att de lämnas till skyddspolisen. I momentet tar lagstiftaren inte ställning till på vilket konkret sätt försvarsmaktens underrättelsetjänst ska lämna data till skyddspolisen. I regel kommer data att lämnas via en krypterad dataförbindelse, men bestämmelsen ska också göra det möjligt att de lämnas på något annat tillräckligt informationssäkert sätt.

På skyddspolisens övriga samarbete med militärunderrättelsemyndigheten tillämpas enligt 4 mom. 5 a kap. 54 § i polislagen. Med det övriga samarbetet avses annat samarbete rörande underrättelseinhämtning som avser datatrafik än det tekniska genomförande av underrättelseinhämtningen som det föreskrivs om i 1–3 mom. och som försvarsmaktens underrättelsetjänst sköter på uppdrag av skyddspolisen. Eftersom militärunderrättelsemyndigheten till skillnad från 1–3 mom. nämns i detta moment, är det möjligt att bedriva det samarbete som avses i momentet även med andra militärunderrättelsemyndigheter än försvarsmaktens underrättelsetjänst. Enligt 8 § i den föreslagna lagen om militär underrättelseverksamhet är militärunderrättelsemyndigheterna huvudstaben och försvarsmaktens underrättelsetjänst.

Enligt det föreslagna 5 a kap. 54 § 1 mom. i polislagen ska skyddspolisen samarbeta med militärunderrättelsemyndigheten för att sköta underrättelseinhämtningen på ett ändamålsenligt sätt och i detta syfte, trots det som föreskrivs om sekretess, ge militärunderrättelsemyndigheten behövliga uppgifter. Enligt 2 mom. i samma paragraf får närmare bestämmelser om samarbetet mellan skyddspolisen och militärunderrättelsemyndigheten utfärdas genom förordning av statsrådet.

Eftersom innehållet i det moment som det är fråga om här utgörs av en hänvisning till den paragraf i 5 a kap. i polislagen som nämns ovan, hänvisas i fråga om motiveringarna till momentet utöver det som sagts ovan till motiveringarna till den aktuella paragrafen i polislagen.

11 §. *Beräkning av tidsfrister.* I paragrafen föreskrivs det om hur de tidsfrister som avses i lagen ska beräknas.

Eftersom paragrafen till sitt sakinnehåll motsvarar bestämmelserna i den gällande 5 kap. 49 § och den föreslagna 5 a kap. 40 § i polislagen, hänvisas för detaljmotiveringen till paragrafen till dessa paragrafer i polislagen.

12 §. *Förbud mot underrättelseinhämtning.* I paragrafen ingår ett förbud mot att rikta underrättelseinhämtning som avser datatrafik mot vissa typer av meddelanden och information.

Förbudet mot underrättelseinhämtning ska för det första gälla meddelanden vars avsändare och mottagare fysiskt befinner sig i Finland när kommunikationen äger rum. Underrättelseinhämtning som avser datatrafik är inte ett verktyg för att följa inhemska hot, utan dess syfte är att göra det möjligt att skaffa information om allvarliga yttre hot mot den nationella säkerheten, det vill säga hot vars ursprung finns utanför Finland. Av denna orsak ska underrättelseinhämtningen i överensstämmelse med definitionen i 2 § riktas endast mot sådan datatrafik som överskrider Finlands gräns i ett kommunikationsnät. Att det är nödvändigt att särskilt lagstifta om ett förbud mot underrättelseinhämtning riktad mot inhemsk kommunikation sammanhänger med att det faktum att datatrafiken fysiskt överskrider Finlands gräns inte är en garanti för att datatrafiken verkligen har internationell karaktär. Internet har konstruerats så kommunikationen mellan två parter i Finland vid störningar och överbelastning i nätet kan dirigeras via en utländsk nätverksenhet. I sådana fall ser trafiken, när den betraktas på överföringssystemets nivå, ut som gränsöverskridande datatrafik, även om det i verkligheten handlar om inhemsk datatrafik. Syftet med förbudet mot underrättelseinhämtning är att säkerställa att underrättelseinhämtning som avser datatrafik inte riktas mot meddelanden mellan parter som befinner sig i Finland när kommunikationen äger rum när meddelandena på grund av tekniska omständigheter dirigeras från sändaren till mottagaren via utlandet.

Det är i och för sig möjligt att även meddelanden mellan parter som befinner sig i Finland innehåller information som är betydelsefull med avseende på allvarliga yttre hot mot den nationella säkerheten. På grund av att underrättelseinhämtning som avser datatrafik till sin karaktär avviker från övriga metoder för underrättelseinhämtning måste dess användningsområde emellertid begränsas på olika sätt för att säkerställa att en åtgärd som inkräktar på hemligheten i fråga om förtroliga meddelanden alltid har godkänts och sker i så liten utsträckning som möjligt. Eftersom den inhemska kommunikationen bedöms ha en avgjort mindre betydelse än den internationella med hänsyn till inhämtandet av information om de hot, om vilka det enligt förslaget föreskrivs i 3 §, är det befogat att göra gränsdragningen så att den inhemska kommunikationen lämnas helt utanför underrättelseinhämtningen. Utredningen av innehåll och andra uppgifter i inhemska meddelanden i spaningssyfte ska inte baseras på underrättelseinhämtning som avser datatrafik utan på metoder som anges i 5 a kap. i polislagen, däribland teleavlyssning och teleövervakning. Bestämmelser om ett motsvarande förbud mot underrättelseinhämtning som gäller inhemska meddelanden finns till exempel i 2 a § i den svenska signalspaningslagen och i 38 § 2 mom. i den schweiziska spaningslagen.

För att säkerställa att förbudet mot underrättelseinhämtning som riktar sig mot inhemsk kommunikation ska det enligt förslaget i 15 § 1 mom. 1 punkten föreskrivas om en skyldighet att utan dröjsmål utplåna sådan trafik. Att föreskriva om skyldigheten att förstöra data från trafiken är nödvändigt därför att det oftast inte är möjligt att på ett tillförlitligt sätt identifiera inhemsk kommunikation och avskilja den från genuint internationell trafik vid automatiserad avskiljning som utförs med tekniska metoder. Genom att utforma de sökbegrepp som används vid den automatiserade avskiljningen kan man i någon mån minska sannolikheten för att meddelanden mellan inhemska partner hamnar bland automatiskt insamlade data. Sökbegrepp kan likväl inte utformas så att de i samtliga fall kan särskilja genuint internationella meddelanden

från meddelanden mellan inhemska parter som dirigeras via utlandet. På grund av det ovan sagda är det väsentliga innehållet i förbudet mot underrättelseinhämtning som riktar sig mot inhemsk kommunikation skyldigheten att med alla tillgängliga medel förhindra att det i den automatiskt avskilda datatrafiken kommer med inhemsk kommunikation, förbudet mot att utnyttja sådan kommunikation på något som helst sätt samt skyldigheten att förstöra den så snart dess verkliga karaktär blivit klar.

Vid sidan av förbudet mot underrättelseinhämtning som riktar sig mot inhemska meddelanden föreslås ett förbud mot att rikta underrättelseinhämtningen mot kommunikation där avsändaren, mottagaren eller den som upptar kommunikationen har skyldighet eller rätt att vägra vittna med stöd av 17 kap. 13, 14, 16, 20 § eller 22 § 2 mom. i rättegångsbalken.

Enligt 17 kap. 13 § i rättegångsbalken får ett rättegångsombud, ett rättegångsbiträde och en tolk inte olovligen vittna om vad han eller hon har fått veta vid skötseln av ett uppdrag i anslutning till en rättegång, vid lämnande av juridisk rådgivning som gäller huvudmannens rättsliga ställning vid förundersökning eller i någon annan handläggningsfas inför en rättegång eller vid lämnande av juridisk rådgivning som gäller inledande eller undvikande av rättegång. Dessutom föreskrivs det i paragrafen om skyldigheten för en advokat och ett rättegångsbiträde som avses i lagen om rättegångsbiträden med tillstånd att inte olovligen vittna om en enskild persons eller en familjs hemlighet eller affärs- eller yrkeshemligheter som han eller hon har fått kännedom om i något annat uppdrag än ett sådant som avses ovan.

Enligt 17 kap. 14 § i rättegångsbalken får en läkare eller någon annan yrkesutbildad person inom hälso- och sjukvården inte vittna om känsliga uppgifter om en enskild persons eller familjs hälsotillstånd eller någon annan hemlighet som gäller en enskild person eller familj och som han eller hon har fått kännedom om på grund av sin ställning eller uppgift, om inte den till vars förmån tystnadsplikten har föreskrivits ger sitt samtycke till det.

Enligt 17 kap. 16 § i rättegångsbalken får en präst eller någon annan person i motsvarande ställning inte vittna om vad han eller hon har fått veta under bikt eller enskild själavård, om inte den till vars förmån tystnadsplikten har föreskrivits ger sitt samtycke till det.

När ett meddelande enligt lagen om yttrandefrihet i masskommunikation har gjorts tillgängligt för allmänheten, får meddelandets upphovsman, utgivaren och utövaren av programverksamheten enligt 17 kap. 20 § i rättegångsbalken vägra vittna om vem som har lämnat de upplysningar som meddelandet grundar sig på samt om upphovsmannens identitet.

I 17 kap. 22 § 2 mom. i rättegångsbalken utvidgas tillämpningen av en del av de förbud mot att vittna och rättigheter att inte vittna som nämns ovan till fler personer. Enligt momentet har den person som har fått information som avses i 11 § 2 eller 3 mom., 13 § 1 eller 3 mom., 14 § 1 mom. eller 20 § 1 mom. när han eller hon var anställd hos eller annars biträdde den som avses i bestämmelsen i fråga motsvarande skyldighet eller rätt att vägra vittna som den som avses i bestämmelsen i fråga. Hänvisningen till 11 § 2 och 3 mom. i 22 § 2 mom. i rättegångsbalken är inte relevant här, eftersom det inte föreslås att det ska föreskrivas om ett uttryckligt förbud mot underrättelseinhämtning i anslutning till 11 § i rättegångsbalken.

De föreslagna förbud mot underrättelseinhämtning som anknyter till rättegångsbalken har beröringspunkter med men uppvisar också betydande avvikelser från förbuden mot avlyssning och observation i 5 kap. 50 § i polislagen och 10 kap. 52 § i tvångsmedelslagen. Enligt dessa förbud får polisen inte rikta vissa telespaningsmetoder och tekniska metoder för inhämtande av information bland annat mot meddelanden mellan en misstänkt och hans eller hennes rättsliga biträde, meddelanden mellan en misstänkt och en i rättegångsbalken avsedd präst eller meddelanden mellan en misstänkt som berövats sin frihet på grund av brott och en läkare, en

sjukskötare, en psykolog eller en socialarbetare och i allmänhet inte heller meddelanden mellan en misstänkt och en sådan upphovsman till eller utgivare av ett meddelande som gjorts tillgängligt för allmänheten eller utövare av programverksamhet. Förbuden i polislagen och tvångsmedelslagen som rör brottsbekämpningsmetoder gäller följaktligen all telekommunikation och annan motsvarande kommunikation mellan en misstänkt och en person som står i sådan relation till denne som avses i rättegångsbalken oavsett om innehållet i ett enskilt meddelande mellan parterna är sådant att det omfattas av ett förbud mot att vittna eller en rätt att låta bli att vittna i rättegångsbalken.

Med avvikelse från de hemliga metoder för informationsinhämtning och tvångsmedel som regleras genom polislagen och tvångsmedelslagen ska underrättelseinhämtning som avser datatrafik inte riktas mot misstänkta eller förmodade framtida gärningsmän. I fråga om underrättelseinhämtning som avser datatrafik kan omfånget av förbudet mot underrättelseinhämtning följaktligen inte på ett ändamålsenligt sätt anges utgående från kommunikationen mellan en misstänkt och en yrkesutbildad person som avses i rättegångsbalken. I underrättelseinhämtning som avser datatrafik är det i allmänhet inte fråga om att följa någon på förhand identifierad persons kommunikation, utan det handlar om att identifiera hot genom att använda sökbegrepp för automatiserad avskiljning av datatrafik. Ett förbud mot underrättelseinhämtning som avser datatrafik kan inte definieras så att det gäller en persons kontakter till personer i en viss ställning, eftersom en likadan exakt målperson som till exempel vid teleavlyssning ofta inte ens existerar. Därför föreslås det att förbudet mot underrättelseinhämtning som avser datatrafik ska gälla endast de uttryckliga uppgifter om vilka de yrkesutbildade personer som avses i bestämmelsen enligt rättegångsbalken är skyldiga eller har rätt att inte vittna.

Ett enskilt meddelande mellan en yrkesutbildad person enligt rättegångsbalken och den andra parten kan innehålla såväl information som omfattas av förbudet mot att vittna som rätten att låta bli att vittna som annan information. Förbudet mot underrättelseinhämtning ska enligt vad som sagts ovan gälla endast de först nämnda uppgifterna. Övrig information i ett meddelande får göras till föremål för underrättelseinhämtning och lagras om den har betydelse vid den utredning av ett hot för vilken tillstånd för underrättelseinhämtning som avser datatrafik har beviljats. Om informationen saknar betydelse vid utredningen av hotet ska den utplånas. Skyldigheten att utplåna oväsentlig information grundar sig på den uttryckliga bestämmelsen i 15 § 1 mom. 3 punkten i den föreslagna lagen.

I bestämmelsen nämns såväl avsändaren och mottagaren av informationen, det vill säga parterna vid kommunikation mellan två eller fler parter, som den som upptar informationen. Med den som upptar information avses den person som sparar information, till exempel en handling, med användning av en molntjänst. Om innehållet i en sådan handling som sparats med hjälp av en molntjänst omfattas av ett förbud mot att vittna eller en rätt att låta bli att vittna som nämns i paragrafen, åtnjuter det skydd mot underrättelseinhämtning med stöd av förbudet.

Att iaktta det aktuella förbudet mot underrättelseinhämtning på ett sådant sätt att information som omfattas av förbudet inte alls samlas in är teknisk omöjligt. Det första steget i underrättelseinhämtning som avser datatrafik grundar sig på automatiserad avskiljning med användning av sökbegrepp. Bortsett från de undantag som anges i 4 § 2 mom. ska sökbegrepp inte få gälla innehållet i ett meddelande. Eftersom tillämpligheten hos förbudet mot underrättelseinhämtning bestäms utifrån innehållet i informationen, kan man i praktiken avgöra om informationen omfattas av förbudet först i samband med att innehållet i meddelandet utreds manuellt. Problemet i sig är inte nytt, och det rör inte bara underrättelseinhämtning som avser datatrafik. Det är inte heller alltid möjligt att bokstavligen iaktta förbuden mot avlyssning och observation enligt polislagen och tvångsmedelslagen, eftersom det att ett meddelande omfattas av förbudet mot avlyssning kan framgå först medan avlyssningen pågår (10 kap, 52 § 2 mom. i

tvångsmedelslagen och 5 kap. 50 § i polislagen som innehåller en hänvisning till det momentet). På grund av det som sagts ovan anges det i den föreslagna 15 § en skyldighet att utplåna information. Genom denna säkerställs att behandlingen av information som omfattas av ett förbud mot underrättelseinhämtning utan dröjsmål avslutas och denna information omedelbart utplånas när dess karaktär av sådan information kommer fram.

13 §. *Granskning av upptagningar och handlingar.* Enligt paragrafen ska en i 5 kap. 7 § i polislagen avsedd polisman som hör till befälet vid skyddspolisen eller en av denne förordnad tjänsteman utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av underrättelseinhämtning som avser datatrafik.

Eftersom paragrafen till sitt sakinnehåll motsvarar bestämmelserna i gällande 5 kap. 51 § och det föreslagna 5 a kap. 42 § i polislagen, hänvisas i fråga om detaljmotiveringen till paragrafen till detaljmotiveringarna till dessa paragrafer i polislagen.

14 §. *Undersökning av upptagningar.* Enligt paragrafen får upptagningar som uppkommit vid användningen av underrättelseinhämtning som avser datatrafik undersökas endast av domstol och en polisman som hör till befälet vid skyddspolisen. Enligt förordnande av en polisman som hör till befälet vid skyddspolisen eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en expert eller av någon annan som anlitas för inhämtande av information.

Eftersom paragrafen till sitt sakinnehåll motsvarar bestämmelserna i gällande 5 kap. 52 § och det föreslagna 5 a kap. 43 § i polislagen, hänvisas i fråga om detaljmotiveringen till paragrafen till dessa paragrafer i polislagen.

15 §. *Utplåning av information.* I paragrafen föreskrivs det om skyldigheten att utan dröjsmål utplåna vissa slag av information som inhämtats genom underrättelseinhämtning som avser datatrafik. Skyldigheten att utplåna information ska gälla dels sådan information som omfattas av det förbud mot underrättelseinhämtning som föreslås i 12 §, dels information som inte behövs för tryggandet av den nationella säkerheten. Skyldigheten att förstöra information som omfattas av ett förbud mot underrättelseinhämtning och det förbud mot att utnyttja informationen på något sätt som följer av denna skyldighet är absoluta och avsteg från dem är inte tillåtna. Skyldigheten att förstöra information som är oväsentlig med hänsyn till tryggandet av den nationella säkerheten är däremot enligt förslaget inte absolut, utan avsteg kan göras av skäl som specificeras i paragrafen.

Enligt 1 mom. 1 punkten i paragrafen ska information som inhämtats genom underrättelseinhämtning som avser datatrafik utplånas utan dröjsmål om det visar sig att båda parterna i kommunikationen befann sig i Finland när kommunikationen försiggick. Skyldigheten kompletterar det förbud mot underrättelseinhämtning som föreslås i 12 §. Enligt den paragrafen får underrättelseinhämtning som avser datatrafik inte riktas mot ett meddelande vars avsändare och mottagare befinner sig i Finland (ett ”inhemskt meddelande”). I den mån detta slags meddelanden som omfattas av ett förbud mot underrättelseinhämtning trots allt filtreras ut för behandling, ska de enligt den bestämmelse som det är fråga här förstöras utan dröjsmål när det blivit klart att de till sin karaktär är inhemska meddelanden.

Den praktiska betydelsen av skyldigheten att förstöra meddelandena understryks av det faktum att det inte är tekniskt omöjligt att till fullo iaktta förbudet enligt 12 § mot underrättelseinhämtning som riktar sig mot inhemsk kommunikation. Ett meddelande kan dirigeras till mottagaren via utlandet, det vill säga så att det passerar över Finlands gräns även om såväl avsändaren som mottagaren de facto befinner sig i Finland. Genom utformningen av de sökbegrepp som används vid den automatiserade avskiljningen kan man i någon mån minska sanno-

likheten för att meddelanden mellan inhemska parter hamnar bland automatiskt insamlade data. Risken kan likväl i allmänhet inte helt elimineras, varför även inhemska meddelanden kan bli föremål för den manuella behandling som avses i 5 §. Vid den manuella behandlingen kan meddelandets inhemska natur framgå redan vid granskningen av meddelandets styr- och förmedlingsdata, i vilket fall meddelandet måste förstöras utan dröjsmål och utan att dess innehåll utreds. I vissa fall framgår meddelandets inhemska natur först när dess innehåll utreds manuellt. I sådana fall ska utredningen avslutas omedelbart och meddelandet förstöras utan dröjsmål.

Enligt 2 punkten ska information som inhämtats genom underrättelseinhämtning som avser datatrafik utplånas utan dröjsmål om det framgår att avsändaren, mottagaren eller den som upptar kommunikationen har skyldighet eller rätt att vägra vittna om informationen på det sätt som avses i 12 §. Skyldigheten att utplåna informationen gäller i överensstämmelse med hänvisningen i 12 § information som avses i 17 kap. 13, 14, 16 och 20 § samt 22 § 2 mom. i rättegångsbalken och som de yrkesutbildade personer som avses i bestämmelserna i fråga är skyldiga eller har rätt att inte vittna om. Skyldigheten att utplåna informationen ska inte gälla all kommunikation som de yrkesutbildade personerna i fråga deltar i, utan den avgörs enligt innehållet i informationen. Även om det inte enligt den aktuella punkten finns någon skyldighet att förstöra den information som ingår i en yrkesutbildad persons kommunikation, kan en sådan skyldighet föreligga med stöd av 1 punkten som behandlats ovan eller 3 punkten som behandlas nedan.

I bestämmelsen nämns såväl avsändaren och mottagaren av informationen, det vill säga parterna vid kommunikation mellan två eller fler parter, som den som upptar informationen. Med den som upptar information avses den person som sparar information, till exempel en handling, med användning av en molntjänst. Om innehållet i ett dokument som sparas i en molntjänst omfattas av något av förbuden mot att vittna eller någon av rättigheterna att inte vittna i bestämmelsen, ska det förstöras.

Informationen ska förstöras utan dröjsmål när det visat sig att det omfattas av ett förbud mot underrättelseinhämtning enligt rättegångsbalken. Av orsaker som lagts fram i detaljmotiveringen till 12 § ovan sker detta i regel först när innehållet utreds i enlighet med den föreslagna 6 §. Med skyldigheten att utan dröjsmål utplåna information avses i sådana fall att en ingående utredning av information som omfattas av ett förbud mot att vittna eller rätten att låta bli att vittna omedelbart ska avslutas och informationen samt eventuella anteckningar om den förstöras.

Enligt 3 punkten ska information som inhämtats genom underrättelseinhämtning som avser datatrafik utplånas utan dröjsmål om det visar sig att informationen inte behövs för att skydda den nationella säkerheten. Den skyldighet att utplåna informationen som avses i bestämmelsen gäller följaktligen information som är oväsentlig med hänsyn till tryggandet av den nationella säkerheten.

Information som inhämtats genom underrättelseinhämtning som avser datatrafik kan sannolikt i vissa fall gälla annan verksamhet som allvarligt hotar den nationella säkerheten än den som tillståndet för underrättelseinhämtning beviljats för. Det kan till exempel vara fråga om att tillstånd för underrättelseinhämtning som avser datatrafik har beviljats för inhämtande av information om ett hot som sammanhänger med terrorism och att underrättelseinhämtning som bedrivs enligt tillståndet vid sidan av eller i stället för terrorismen ger information om massförstörelsevapen. Om detta slags information som inhämtats som biprodukt vid tillåten underrättelseinhämtning har betydelse när det gäller tryggandet av den nationella säkerheten, finns det ingen skyldighet att utplåna den.

Eftersom bestämmelsen motsvarar det föreslagna 5 a kap. 45 § 1 mom. i polislagen, hänvisas i övrigt till motiveringarna till den bestämmelsen.

Enligt 2 mom. kan information som avses i 1 mom. 3 punkten dock överlämnas för brottsbekämpning i enlighet med de förutsättningar som föreskrivs i 5 a kap. 45 § i polislagen samt bevaras och lagras i ett register som avses i lagen om behandling av personuppgifter i polisens verksamhet i enlighet med de förutsättningar som föreskrivs i 5 a kap. 44 § 2 mom. i polislagen. Det är fråga om en bestämmelse om undantag under vissa villkor från skyldighet att utplåna information och det därmed förknippade förbudet mot att använda informationen. På det sätt som framgår av bestämmelsen ska det vara möjligt att göra avsteg från skyldigheten att utplåna information och förbudet mot att använda informationen endast när skyldigheten i enlighet med 1 mom. 3 punkten grundar sig på att informationen inte behövs för att trygga den nationella säkerheten. Om skyldigheten att utplåna informationen i stället beror på att det är fråga om inhemsk kommunikation (1 mom. 1 punkten) eller information som omfattas av e skyldighet eller rätt att vägra vittna (1 mom. 2 punkten), är det inte på grund av 2 mom. eller av andra orsaker möjligt att göra avsteg från skyldigheten att utplåna information och det förbud mot att använda informationen som följer av den.

Eftersom innehållet i det föreslagna momentet utgörs av hänvisningar till 5 a kap. 45 § och 45 § 2 mom. i polislagen, hänvisas i övrigt till motiveringarna till dessa bestämmelser.

För utplåning av informationen ansvarar enligt 3 mom. den tekniska utföraren av underrättelseinhämtning som avser datatrafik eller uppdragsgivaren i det fall att informationen redan har lämnats till uppdragsgivaren. Genom bestämmelsen säkerställs det att meddelandena och informationen förstörs utan dröjsmål på försorg av den myndighet som har observerat att de omfattas av den skyldighet som anges i paragrafen.

Den tekniska utföraren av underrättelseinhämtning som avser datatrafik är enligt 10 § 1 mom. försvarsmaktens underrättelsetjänst. Som teknisk utförare överlämnar försvarsmaktens underrättelsetjänst den information som den samlat in inom ramen för sitt uppdrag till skyddspolisen i obearbetad form. Den har inte rätt att utreda innehållet i meddelandena och inte heller granska andra uppgifter i den datatrafik som samlas in utöver vad det tekniska utförandet av uppdraget kräver. I det tekniska genomförandet är det därför troligen i allmänhet inte möjligt att se om det material som samlats in på grundval av uppdraget innehåller meddelanden eller information som omfattas av skyldigheten att förstöra information. En sådan karaktär hos meddelanden och information kan i regel observeras först i samband med den fortsatta behandlingen enligt 6 § av den automatiskt avskilda datatrafiken. Enligt förslaget utförs den av skyddspolisen. I praktiken bedöms det alltså bli mycket ovanligt att meddelanden och information förstörs av försvarsmaktens underrättelsetjänst och inte överlämnas till skyddspolisen.

Syftet med att meddelanden och information förstörs är att säkerställa att de inte på något sätt kan utnyttjas i underrättelsemyndighetens verksamhet. Av det att meddelanden och information utplånas följer emellertid inte att det inte bevaras några anteckningar om dem i dokument. Av skäl som sammanhänger med laglighetsövervakningen och rättssäkerheten är det nödvändigt att varje utplåning och grunden för den dokumenteras i tillräcklig omfattning. Bestämmelser om hur och med vilken noggrannhet utplåningen av meddelanden och information registreras ska enligt 23 § utfärdas genom förordning av statsrådet.

16 §. *Utlämnande av information om skadliga datorprogram eller skadliga datorkommandon till myndigheterna, företag eller sammanslutningar.* I paragrafen föreskrivs det om skyddspolisens rätt att trots sekretessbestämmelserna lämna ut sådan information som inhämtats med hjälp av underrättelseinhämtning som avser datatrafik och som gäller skadliga datorprogram eller skadliga datorkommandon till myndigheter, företag eller sammanslutningar, om utläm-

nandet av informationen behövs för att skydda den nationella säkerheten eller informationsmottagarens intressen.

Ett av syftena med underrättelseinhämtningen är att förbättra skyddet av samhället mot tekniskt avancerade attacker via datanät, såsom cyberspionage. Den bedöms resultera i en stor mängd observationer och kunskap om datorprogram och datorkommandon som används vid attacker i datanät. Eftersom avancerade attacker i datanät kan rikta sig mot såväl myndigheter som privata aktörer, är det viktigt med hänsyn till skyddet av samhället som helhet att information om skadeprogram som används för sådana attacker i så hög grad som möjligt kan lämnas till potentiella mål för attackerna. Genom att lagstifta om rätten att lämna ut informationen kan man bidra till att trygga informationsmottagarens möjligheter att vidta sådana åtgärder för att sköta sin informationssäkerhet som det föreskriv om i 272 § i lagen om tjänster inom elektronisk kommunikation. Åtgärder enligt bestämmelsen i fråga kan bland annat inbegripa automatisk utredning av innehållet i meddelanden, automatiskt förhindrande eller automatisk begränsning av förmedling eller mottagning av meddelanden och automatisk borttagning av skadliga datorprogram som äventyrar informationssäkerheten från meddelanden.

Enligt 1 mom. får information om skadliga datorprogram eller skadliga datorkommandon lämnas ut trots sekretessbestämmelserna. Sådan information kan uppenbarligen vara sekretessbelagd närmast enligt 24 § 1 mom. 7 och 9 punkten i lagen om offentlighet i myndigheternas verksamhet (621/1999). Till den sekretessbelagda informationen hör bland annat handlingar som gäller skyddsarrangemang för data- och kommunikationssystem och genomförandet av arrangemangen, om det inte är uppenbart att utlämnandet av uppgifter ur en sådan handling inte äventyrar genomförandet av syftet med skyddsarrangemangen, Att information om ett skadligt datorprogram eller datorkommando blir offentlig kan åtminstone i vissa fall äventyra att syftet med vissa säkerhetsåtgärder nås, eftersom den aktör som använder programmet eller kommandot då skulle kunna dra slutsatser om myndigheternas förmåga att upptäcka och avvärja attacker. Det här kan i sin tur leda till att programmet eller kommandot i fråga ändras eller vidareutvecklas så att det blir ännu svårare att upptäcka. Eftersom ett modifierat skadeprogram kan användas även i sådan verksamhet som direkt äventyrar statens säkerhet, kan en grund för sekretess också vara 24 § 1 mom. 9 punkten i lagen om offentlighet i myndigheternas verksamhet. Enligt bestämmelsen i fråga är skyddspolisens och andra myndigheters handlingar som gäller upprätthållande av statens säkerhet sekretessbelagda, om det inte är uppenbart att utlämnandet av uppgifter ur dessa inte äventyrar statens säkerhet. Även om offentliggörandet av information om ett skadeprogram skulle skada intressen som nämnts ovan, skadar utlämnandet av informationen till en enskild organisation som är föremål för en attack genom ett datanät inte nödvändigtvis dessa intressen. I så fall kan uppgifterna lämnas ut till organisationen för att värna den nationella säkerheten eller organisationens intressen.

Bestämmelsen är till sin natur tillåtande, inte bindande. Beslutsfattandet som gäller utlämnande av uppgifter ska enligt förslaget grunda sig fallspecifik prövning samt intresseavvägning. I vissa situationer kan orsaker som sammanhänger med den nationella säkerheten utgöra ett hinder för att lämna ut information även om det i sig skulle vara viktigt för myndigheten, företaget eller sammanslutningen att få informationen för att kunna säkra sina intressen. Det är klart att de orsaker som anknyter till den nationella säkerheten bara i undantagsfall kan utgöra ett hinder för utlämnande till en myndighetsaktör, eftersom det tvärt om för att trygga den nationella säkerheten i allmänhet är nödvändigt att myndigheten får sådan information. Intresseavvägningen har större betydelse när informationsmottagaren är en privat aktör. Även om det finns skäl att tillämpa en låg tröskel för utlämnande även till en privat aktör, bör det poängteras att syftet med bestämmelsen inte är att överföra ansvar för företagens och sammanslutningarnas informationsskydd till skyddspolisen. Syftet med bestämmelsen är att göra det möjligt för skyddspolisen att för sin del stödja företagens och sammanslutningarnas åtgärder för att skydda sig mot nätattacker.

Det finns två alternativa motiveringar till att lämna ut information om ett skadligt datorprogram eller datorkommando: att värna den nationella säkerheten och att skydda informationsmottagarens intressen. Dessa grunder för att utlämna informationen kan sammanfalla om informationsmottagaren är en myndighet eller till exempel ett företag eller en sammanslutning som har stor betydelse för upprätthållandet av sådan infrastruktur som är livsviktig för hela samhällsekonomin. Av det att grunderna är alternativa följer likväl att informationen inom ramen för den prövning som beskrivs ovan kan lämnas ut oavsett om företaget eller sammanslutningen har sådan betydelse eller inte.

På tystnadsplikten för den som är anställd av ett företag eller en sammanslutning ska enligt 2 mom. tillämpas i 23 § 2 mom. i lagen om offentlighet i myndigheternas verksamhet. Enligt andra meningen i det momentet gäller tystnadsplikten den till vilken en myndighet inom ramen för en sekretessbestämmelse som innehåller en offentlighets- eller sekretesspresumtion har meddelat uppgifter som allmänheten inte ska ha tillgång till. Av 23 § 1 mom. i lagen om offentlighet i myndigheternas verksamhet följer för anställda hos ett företag eller en sammanslutning att de inte får röja en handlings sekretessbelagda innehåll eller en uppgift som vore sekretessbelagd om den ingick i en handling, och inte heller någon annan omständighet som de har fått kännedom om i samband med sin verksamhet och för vilken tystnadsplikt föreskrivs genom lag. Information som omfattas av tystnadsplikt får inte heller röjas efter det att verksamheten vid företaget eller sammanslutningen har upphört.

17 §. *Utlämnande av information för brottsbekämpning.* På utlämnade av information för brottsbekämpning tillämpas enligt paragrafen 5 a kap. 44 § i polislagen.

För motiveringar till paragrafen hänvisas till motiveringarna till den föreslagna paragrafen i polislagen.

18 §. *Begränsning av partsoffentlighet i vissa fall.* I paragrafen föreskrivs det om begränsning av en parts rätt att få information i ärenden som gäller underrättelseinhämtning som avser datatrafik.

Eftersom paragrafen till sitt sakinnehåll motsvarar bestämmelserna i den föreslagna 5 a kap. 49 § i polislagen, hänvisas för motiveringar till paragrafen till motiveringarna till den paragrafen i polislagen.

19 §. *Protokoll.* Enligt paragrafen ska det efter att användning av underrättelseinhämtning som avser datatrafik upphört utan ogrundat dröjsmål upprättas ett protokoll.

Eftersom paragrafen till sitt sakinnehåll motsvarar bestämmelserna i gällande 5 kap. 59 § och det föreslagna 5 a kap. 48 § i polislagen, hänvisas i fråga om motiveringar till paragrafen till dessa paragrafer i polislagen.

20 §. *Underrättelse om underrättelseinhämtning som avser datatrafik.* I paragrafen föreskrivs det om att underrätta om underrättelseinhämtning som avser datatrafik. Så som framgår av den allmänna motiveringen har Europadomstolen i många av sina avgöranden tagit ställning till frågan om och i vilka situationer en person som är föremål för underrättelseinhämtning ska ha rätt att bli informerad av en myndighet om den spaningsåtgärd, till exempel underrättelseinhämtning som avser datatrafik, som han eller hon blivit föremål för. Domstolen har i sin avgörandepraxis understrukit att föremålet för informationsinhämtningen ska ha tillgång till effektiva rättssäkerhetsinstrument mot myndigheters eventuellt lagstridiga informationsinhämtning. En förutsättning för användning av möjligheten att anföra klagomål är enligt domstolen i allmänhet att personen får information av myndigheten om den informationsinhämtning som han eller hon blivit föremål för efter det att användningen av den hemliga metoden för informat-

ionsinhämtning har avslutats. Enligt domstolens avgörandepraxis följer det likväl inte av detta att underrättelsen måste göras omedelbart efter att informationsinhämtningen avslutats. Hotet om vilket information har skaffats med hjälp av informationsinhämtningsmetoden kan fortsätta i år eller till och med årtionden. I sådana fall är det nödvändigt att skjuta upp underrättelsen i motsvarande grad för att skydda säkerhetsmyndigheternas verksamhet. För att göra det möjligt att använda ett rättsmedel ska underrättelsen likväl göras så snart det inte längre finns någon individuell grund för att inte göra den. Emellertid kan också ett system som inte kräver att personen som varit föremål för informationsinhämtningen informeras vara förenligt med konventionen om de mänskliga rättigheterna. I så fall ska rätten att anföra klagomål mot myndighetens hemliga informationsinhämtning enligt nationell lagstiftning vara så generell att vem som helst får klaga redan på den grund att personen misstänker att en myndighet har kränkt det skydd som hans eller hennes konfidentiella kommunikation åtnjuter (EDMR Kennedy mot Förenade kungariket).

I den föreslagna paragrafen begränsas skyldigheten att underrätta om underrättelseinhämtning som avser datatrafik till fall där underrättelseinhämtningen kan ses som en relativt allvarlig kränkning av hemligheten i fråga om förtroliga meddelanden. Som en motvikt mot den begränsade underrättelseskyldigheten enligt paragrafen föreslås det att det i 22 § i lagen om övervakning av underrättelseverksamheten föreskrivs om en allmän rätt att lämna en begäran om utredning av underrättelseinhämtning som avser datatrafik till den myndighet som sköter den rättsliga övervakningen av underrättelseinhämtningen. Den föreslagna underrättelseskyldigheten är mera omfattande än till exempel den svenska, där underrättelseskyldigheten enligt 11 a § i signalspaningslagen gäller bara om det vid signalspaning har använts sökbegrepp som direkt kan hänföras till en viss fysisk person.

Om innehållet i ett konfidentiellt meddelande som sänts av eller information som lagrats av en person som befinner sig i Finland har klarlagts manuellt vid sådan fortsatt behandling av automatiskt avskild information som avses i 6 §, ska personen enligt första meningen i paragrafen underrättas om underrättelseinhämtning som avser datatrafik med iakttagande av bestämmelserna om underrättelse om teleavlyssning i 5 a kap. 47 § i polislagen. Skyldighet att underrätta föreligger emellertid inte, om den information som inhämtats med underrättelseinhämtning som avser datatrafik har utplånats med stöd av 9 § 2 mom. eller 15 §.

Information som samlats in med hjälp av automatiserad avskiljning ska enligt 6 § får behandlas automatiskt och manuellt. Vid automatisk och manuell behandling får man utreda meddelandets innehåll och annan konfidentiell information. I den paragraf som det nu är fråga om krävs det att den som är föremål för underrättelseinhämtning underrättas när behandlingen varit manuell och inneburit att innehållet i ett förtroligt meddelande eller lagrad information klarlagts. Eftersom en främmande stats eller med en sådan jämställbar aktörs kommunikation enligt motiveringen till 4 § inte omfattas av skyddet av hemligheten i fråga om förtroliga meddelanden, utgör bestämmelsen ingen grund för en skyldighet att underrätta om underrättelseinhämtning som avser datatrafik till en part i sådan kommunikation. Bestämmelsen utgör inte heller någon grund för en skyldighet att underrätta en sådan person som i sig åtnjuter skydd för hemligheten i fråga om förtroliga meddelanden men som inte befinner sig i Finland om underrättelseinhämtning som avser datatrafik. En skyldighet att underrätta är i dessa fall ofta även i övrigt ineffektiv på grund av bristande kännedom om personens identitet eller därför att personens vistelseort är obekant och inte kan utredas med en skälig arbetsinsats även om personens identitet är bekant.

Utöver innehållet i förtroliga meddelanden nämns innehållet i lagrad information särskilt i bestämmelsen. Med lagrad information avses information som lagrats genom en molntjänst.

När en skyldighet att underrätta om underrättelseinhämtning som avser datatrafik föreligger, ska bestämmelserna om underrättelse om teleavlyssning i 5 a kap. 47 § i polislagen tillämpas på underrättandet. Sådan underrättelseinhämtning som avser datatrafik och där innehållet i ett konfidentiellt meddelande klarläggs är nära jämförbar med teleavlyssning såväl tekniskt som med hänsyn till hur allvarlig kränkningen av de grundläggande friheterna och rättigheterna. I fråga om skyldigheten att underrätta ska därför enligt förslaget samma regler gälla för de två metoderna. Då man på underrättelse om underrättelseinhämtning som avser datatrafik tillämpar reglerna förunderrättelse om teleavlyssning följer att den som varit föremål för underrättelseinhämtning som avser datatrafik utan dröjsmål ska underrättas om detta skriftligen efter det att syftet med underrättelseinhämtningen har nåtts. Domstolen ska dock på yrkande av en polisman som hör till befälet vid skyddspolisen få besluta att underrättelsen till den som varit föremål för åtgärden får skjutas upp med högst två år åt gången, om det är motiverat för att trygga pågående underrättelseinhämtning, värna den nationella säkerheten eller skydda liv eller hälsa. Domstolen ska få besluta att underrättelsen helt ska utebli, om det är nödvändigt med hänsyn till den nationella säkerheten eller för att skydda liv eller hälsa. Om den som är föremål för inhämtandet av information inte är identifierad vid utgången av den föreskrivna tiden eller uppskovet, ska han eller hon utan ogrundat dröjsmål skriftligen underrättas om underrättelseinhämtningen när identiteten har utretts. Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om underrättelsen. Om skyddspolisen emellertid fortsätter inhämtandet av information med stöd av 5 a kap. 5 § i polislagen, ska bestämmelserna om underrättelse om hemligt inhämtande av information i 5 kap. 58 § i den lagen iakttas. I fråga om handläggning av underrättelseärenden i domstol ska den föreslagna 5 a kap 34 § i polislagen iakttas.

Utöver det som sagts ovan hänvisas till motiveringarna till det föreslagna 5 a kap. 47 § i polislagen.

Enligt den andra meningen i paragrafen föreligger skyldighet att underrätta emellertid inte, om den information som inhämtats med underrättelseinhämtning som avser datatrafik har utplånats med stöd av 9 § 2 mom. eller 15 §. Det är fråga om ett undantag från det som föreskrivs i första meningen. Om innehållet i ett meddelande till eller från en person som befinner sig i Finland har klarlagts genom manuell behandling men det i samband med detta framgått att det är fråga om information som omfattas av skyldigheten att utplåna information och informationen i enlighet med denna skyldighet har utplånats utan dröjsmål, föreligger följaktligen inte skyldighet att underrätta. Skyldigheten att underrätta om underrättelseinhämtning som avser datatrafik kan inte i dessa fall anses motiverad, eftersom innehållet i det förtroliga meddelandet har utplånats och alltså inte längre innehas av utredningsmyndigheten.

21 §. *Genomförande av den koppling som underrättelseinhämtning som avser datatrafik förutsätter.* Vid genomförande av den koppling som underrättelseinhämtning som avser datatrafik förutsätter vid civil underrättelseinhämtning iakttas 72 § i lagen om militär underrättelseverksamhet. Substansbestämmelserna om genomförande av kopplingen ska ingå i lagen om militär underrättelseverksamhet därför att den nära anknyter till det tekniska genomförandet av underrättelseinhämtning som avser datatrafik som försvarsmaktens underrättelsetjänst ska svara för. Med hjälp av denna bestämmelse som innehåller en hänvisning till lagen om militär underrättelseverksamhet säkerställs att den person som genomför kopplingen är skyldig att utföra de åtgärder som personen ansvarar för oavsett om de ska användas för en civil eller en militär underrättelsemyndighets underrättelseinhämtning som avser datatrafik.

Enligt 72 § i lagen om militär underrättelseverksamhet ska den som utför kopplingen vid underrättelseinhämtning som avser datatrafik verkställa de åtgärder som tillstånden i 5 kap. gäller och överlåta datatrafiken i den del av kommunikationsnätet som avses i tillståndet till försvarsmaktens underrättelsetjänst. Till den utförare av kopplingen som avses i paragrafen ut-

ses enligt 9 § i lagen om militär underrättelseverksamhet Suomen Erillisverkot Oy. Av hänvisningen till 72 § i lagen om militär underrättelseverksamhet följer att Suomen Erillisverkot Oy är skyldigt att utföra kopplingen och överlåta datakommunikationen till försvarsmaktens underrättelsetjänst även när det är fråga om verkställigheten av beslut som avses i 7 eller 9 § i den aktuella lagen.

För motiveringar till paragrafen hänvisas i övrigt till motiveringarna till 72 § i lagen om militär underrättelseverksamhet.

22 §. *Dataöverförares skyldighet att lämna uppgifter.* I paragrafen föreskrivs det om dataöverförarens skyldighet att utan obefogat dröjsmål till skyddspolisen på specificerade begäran av en polisman som hör till skyddspolisens befäl lämna sådana tekniska uppgifter om strukturen på det kommunikationsnät som dataöverföraren innehar och som överskrider Finlands gräns och om dirigeringen av datatrafiken i detta nät som behövs för att identifiera en del av ett kommunikationsnät för ett sådant yrkande om tillstånd till domstol eller ett sådant tillståndsbeslut som gäller användning av underrättelseinhämtning som avser datatrafik.

Skyldigheten i fråga anknyter till bestämmelsen i 7 § 2 mom. 5 punkten om domstolens tillstånd enligt vilken skyddspolisen i det tillståndsyrkande som den framlägger för domstolen ska specificera den del av kommunikationsnätet som överskrider Finlands gräns i vilken sökbegreppen för underrättelseinhämtning som avser datatrafik ska jämföras med datatrafiken. För att denna del ska kunna specificeras med tanke på tillståndsyrkan, är det nödvändigt att skyddspolisen får information som underlättar specificeringen av de aktörer som av orsaker som sammanhänger med deras affärsverksamhet innehar sådan information. Genom att lagstifta om skyldigheten att lämna information kan man förebygga att den jämförelse baserad på sökbegrepp som enligt 5 § ska ingå i underrättelseinhämtning som avser datatrafik omfattar en större del av datatrafiken än vad som är nödvändigt för att utreda den verksamhet som allvarligt hotar den nationella säkerheten och som är föremålet för underrättelseinhämtningen. Om dataöverföraren innehar information som visar att den datatrafik som rör den hotande verksamhet som ska utredas inte kan äga rum i en vis del av kommunikationsnätet till exempel därför att den har reserverats för en kundorganisation som är irrelevant med tanke på det hot som utreds, kan delen i fråga inte omfattas av ett yrkande om tillstånd för underrättelseinhämtning som avser datatrafik.

Till den information som informationsskyldigheten enligt paragrafen gäller hör framför allt uppgifter om vilka kundorganisationer som har reserverat kapacitet av dataöverföraren och vilka delar av det kommunikationsnät som överskrider gränsen och som dataöverföraren kontrollerar dessa reservationer gäller. Paragrafen ålägger dataöverföraren att ge uppgifter även om övriga eventuella omständigheter som inverkar på hur datatrafiken sannolikt dirigeras när den överskrider Finlands gräns i en del av nätet som dataöverföraren äger eller kontrollerar. Det bör understrykas att paragrafen ålägger dataöverföraren att lämna uppgifter bara om de kundorganisationer som reserverat kapacitet, men däremot inte om de konsumentkunder som är parter i kommunikationshändelser. Paragrafen ger inte heller i övrigt skyddspolisen rätt att skaffa eller få information om enskilda kommunikationshändelser eller de personer som är parter i dem.

Dataöverföraren är skyldig att ge uppgifterna på skyddspolisens specificerade begäran. Med kravet att begäran ska vara specificerad avses att skyddspolisen i samband med begäran ska ge tillräckliga uppgifter för att dataöverföraren ska kunna bedöma vilken av den information som den förfogar över som behövs för att uppfylla begäran. Begäran kan inte gälla en obestämd informationsmassa, utan skyddspolisen ska i begäran avgränsa det ärende som är föremål för begäran.

Genom paragrafen åläggs dataöverföraren att ge skyddspolisen sådan information som är nödvändig för att specificera den aktuella delen av kommunikationsnätet. Kravet att informationen är nödvändig innebär att dataöverföraren ska ge skyddspolisen alla sådana uppgifter som kan ha betydelse med beaktande av att kommunikationsnätsdelen ska specificeras så precist som möjligt. Av kravet på att uppgifterna ska vara nödvändiga följer emellertid också att dataöverföraren inte är skyldig att ge skyddspolisen sådana uppgifter som den förfogar över men som inte kan ha betydelse för det aktuella ärendet. Den information som dataöverföraren lämnar skyddspolisen till följd av skyldigheten enligt paragrafen inbegriper inte inhämtandet av förmedlingsdata som rör enskilda personer, utan det är uttryckligen fråga om att identifiera en viss del av kommunikationsnätet.

Dataöverförarens skyldighet att ge information gäller endast sådan information som denne redan förfogar över. Den informationsskyldighet som föreslås innebär följaktligen inte att dataöverförarna måste skaffa ny information att lämna skyddspolisen.

Dataöverföraren har tystnadsplikt i fråga om skyddspolisens begäran och sitt svar med anledning av den enligt 23 § 2 mom. och 24 § 1 mom. 5 och 9 punkten i lagen om offentlighet i myndigheternas verksamhet.

23 §. *Ersättningar till dataöverförare.* I paragrafen föreskrivs det om ersättning som betalas dataöverföraren för kostnader som orsakats av utlämningen av uppgifter, om vem som fattar beslut om betalningen och om sökande av ändring.

Enligt 1 mom. har en dataöverförare rätt att få ersättning av statens medel för direkta kostnader som orsakats av att överföraren i enlighet med 22 § har lämnat ut uppgifter. De direkta kostnader som avses i momentet är i huvudsak arbetskraftskostnader. Indirekta kan också de kostnader som föranleds av tekniska anordningar och andra hjälpmedel som eventuellt utnyttjas när informationen sammanställs vara. Beslut om betalning av ersättning fattas av skyddspolisen. Skyddspolisen avgör följaktligen vilka kostnader som är nödvändiga och ska ersättas. Skyddspolisen bestämmer också ersättningens storlek.

Enligt 2 mom. får omprövning av skyddspolisens beslut begäras på det sätt som anges i förvaltningslagen (434/2003). Omprövningsbeslutet får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges förvaltningsprocesslagen (586/1996). Över förvaltningsdomstolens beslut får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd. Momentet motsvarar bestämmelserna i 10 kap. 64 § 2 mom., 5 kap. 62 § 2 mom. i polislagen och den föreslagna 5 a kap. 51 § i polislagen om sökande av ändring i ett beslut av en polisenhet om ersättning som betalas ett teleföretag bland annat för kostnader som orsakats av att företaget lämnat uppgifter.

24 §. *Inrikesförvaltningens övervakning av underrättelseinhämtning som avser datatrafik.* I paragrafen föreskrivs det om den rättsliga övervakningen vid inrikesförvaltningen av användningen av underrättelseinhämtning som avser datatrafik. Till sitt sakinnehåll motsvarar paragrafen 59 § i det föreslagna 5 a kap. i polislagen.

25 §. *Extern övervakning av underrättelseinhämtning som avser datatrafik.* I paragrafen föreskrivs det om extern övervakning av underrättelseinhämtning som avser datatrafik. Till sitt sakinnehåll motsvarar paragrafen det föreslagna 5 a kap. 60 § i polislagen.

26 §. *Anmälningar till underrättelseombudsmannen.* Enligt paragrafen ska skyddspolisen informera underrättelseombudsmannen om de tillstånd och beslut som gäller metoder för underrättelseinhämtning som meddelats med stöd av denna lag så snart som möjligt efter det att till-

ståndet beviljats eller beslutet fattats. Till sitt sakinnehåll motsvarar paragrafen de föreslagna 5 a kap. 61 § 1 mom. i polislagen.

27 §. *Befogenhet att utfärda förordning.* I paragrafen föreskrivs det om ett bemyndigande att utfärda förordningar om ordnandet och övervakningen av användningen av underrättelseinhämtning som avser datatrafik samt om dokumentering av åtgärderna och om de rapporter som ska lämnas för övervakningen. En bestämmelse om bemyndigande att utfärda förordning med samma sakinnehåll finns för närvarande i 5 kap. 65 § i polislagen, där den gäller ordnande av och tillsyn över användningen av i kapitlet avsedda hemliga metoder för inhämtande av information samt om dokumentering av åtgärderna och om de rapporter som ska lämnas för tillsynen. En motsvarande bestämmelse om bemyndigande att utfärda förordning ska enligt förslaget också ingå i 5 a kap. 62 § i polislagen, där den ska gälla de underrättelsemetoder och annan verksamhet som det ska föreskrivas om i kapitlet. När det gäller motiveringar till den aktuella paragrafen hänvisas till motiveringarna till den paragraf i 5 a kap. i polislagen som nämnts ovan till den del den gäller ordnandet och övervakningen av användningen av en underrättelsemetod samt dokumentering av åtgärderna och de rapporter som ska lämnas för övervakningen

1.3 Polisförvaltningslag

10 § *Skyddspolisen.* Det föreslås att 1 kap. 1 § 1 mom. i polislagen ändras så att det blir polisens uppgift att värna den nationella säkerheten. Denna paragraf ska samstämmas med 1 kap. 1 § 1 mom. i polislagen, och den ska preciseras så att det inom polisens organisation i första hand är skyddspolisen som ska sköta värnandet av den nationella säkerheten.

Enligt första meningen i 10 § 1 mom. i gällande polisförvaltningslag har skyddspolisen till uppgift att i enlighet med inrikesministeriets styrning bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet samt att utföra undersökning av sådana brott. Enligt andra meningen ska skyddspolisen även upprätthålla och utveckla en allmän beredskap för att förebygga verksamhet som äventyrar rikets säkerhet.

Enligt lagförslaget ska den första meningen för det första ändras så att det läggs till att skyddspolisen har till uppgift att inhämta information som behövs för att skydda den nationella säkerheten. Genom ändringen preciseras skyddspolisens uppgift så att spaning och inhämtande av information får en större roll vid sidan av den nuvarande förebyggande uppgiften. Dessutom föreslås det att begreppet ”bekämpa” i samma mening byts ut mot begreppet upptäcka, förhindra och avslöja, eftersom begreppet bekämpa även kan anses inbegripa utredning av brott. I lagförslaget föreslås det att skyddspolisen befrias från uppgiften att utreda brott. I slutet av meningen föreslås det av samma orsak att bestämmelsen om att skyddspolisen utför undersökning av brott stryks. Meningen ändras också så att begreppen förehavande och brott kompletteras med verksamhet. Det tillagda begreppet innebär en hänvisning till verksamhet som allvarligt hotar den nationella säkerheten enligt 5 a kap. 3 § i polislagen och 3 § i lagen om civil underrättelseinhämtning avseende datatrafik. Dessutom föreslås det att meningen ändras så att begreppet äventyra byts ut mot hota. Detta är motiverat eftersom begreppet hotande verksamhet används i 5 a kap. 3 § i polislagen och i 3 § i lagen om civil underrättelseinhämtning avseende datatrafik.

Andra meningen i momentet ändras så att begreppet rikets säkerhet ersätts med det modernare begreppet samhällets säkerhet. Meningen ska också ändras så att förhindra kompletteras med upptäcka. Även detta tillägg avspeglar skyddspolisens uppgift att förutom förebyggande verksamhet inhämta information. Enligt förslaget ska meningen också ändras så att begreppet äventyrar ersätts med begreppet hotar i överensstämmelse med hur första meningen ändras.

Enligt 2 mom. bestämmer inrikesministeriet, efter att ha hört Polisstyrelsen, vid behov närmare om samverkan och samarbetet mellan skyddspolisen och andra polisenheter. Ändringen i momentet har samband med den ändring i 1 mom. som innebär att skyddspolisen fråntas sina befogenheter att utföra förundersökningar. Inrikesministeriet ska följaktligen inte längre bestämma vilka kategorier av ärenden som ska undersökas av skyddspolisen. Inrikesministeriet ska likväl bestämma om samverkan och samarbete mellan skyddspolisen och övriga polisenheter. Även om det föreslås att skyddspolisen ska fråntas sina befogenheter i fråga om förundersökning och tvångsmedel, ska den även i fortsättningen vid behov kunna delta i förundersökningar i egenskap av expertmyndighet. Denna uppgift sammanhänger med beslutsfattandet om samverkan och samarbete mellan polisenheter. Eftersom skyddspolisen likväl inte har egentliga undersökningsuppgifter i samband med förundersökningen, ska omnämnandet om att bestämma om undersökningsarrangemang i slutet av momentet tas bort.

15 a §. *Polisbefogenheter.* Till paragrafen fogas ett nytt 3 mom. där det konstateras att en tjänsteman vid skyddspolisen utöver det som föreskrivs i 1 mom. har rätt att använda i 5 a kap. i polislagen avsedda metoder för underrättelseinhämtning för att värna den nationella säkerheten enligt vad som föreskrivs i det kapitlet.

Med uttrycket ”utöver det som föreskrivs i 1 mom.” avses att endast tjänstemän vid skyddspolisen ska ha rätt att använda de befogenheter som avses i 5 a kap i polislagen. Detta framgår också av det föreslagna 5 a kap. i polislagen och motiveringarna till det. I regel ska de befogenheter som nämns i 5 a kap. användas av polismän som är anställda i tjänsteförhållande hos skyddspolisen, men i vissa situationer kan också någon annan än en polisman bli tvungen att bistå eller delvis använda vissa befogenheter. Därför är det motiverat att i ställe för polismän tala om tjänstemän vid skyddspolisen.

Användningen av de befogenheter som avses i momentet ska inte avgränsas geografiskt på samma sätt som i 1 mom., enligt vilket en polisman vid utförandet av sina uppgifter i hela landet har sådana befogenheter som anges i polislagen eller i någon annan lag. Följaktligen ska en tjänsteman vid skyddspolisen i situationer som anges särskilt i lag ha rätt att använda befogenheterna i fråga även vid underrättelseverksamhet som avser utländska förhållanden dock så att 5 a kap. i polislagen iakttas.

Det 2 mom. som fogas till paragrafen är med hänsyn till 1 mom. en specialbestämmelse.

1.4 Lag om behandling av personuppgifter i polisens verksamhet

5 §. *Skyddspolisens funktionella informationssystem.* Paragrafens 2 mom. ska enligt förslaget ändras så att skyddspolisens funktionella informationssystem även kan innehålla uppgifter som skyddspolisen måste behandla för att kunna skydda den nationella säkerheten eller för att kunna avslöja eller utreda brott.

För att sköta sin uppgift ska skyddspolisen föra ett funktionellt informationssystem, där information som är nödvändig med hänsyn till skyddspolisens uppgift lagras och följaktligen uppgifter som inhämtats med stöd av olika befogenheter. Personuppgifter som inhämtats med stöd av befogenheterna enligt de föreslagna 5 a kap. i polislagen och lagen om civil underrättelseinhämtning avseende datatrafik lagras i skyddspolisens funktionella informationssystem. Det föreslås att paragrafen om skyddspolisens funktionella informationssystem ändras så att värnandet av den nationella säkerheten nämns i överensstämmelse med 1 kap. 1 § 1 mom. i polislagen, som enligt förslaget ändras. Som grund tilläggs dessutom av samma orsak avslöjande av brott.

13 §. *Polisens rätt att få uppgifter ur vissa register och informationssystem.* Det föreslås att paragrafens 2, 4, 15 och 16 punkt ändras så att frasen ”för skyddande av den nationella säkerheten” infogas. Förslaget anknyter till den föreslagna ändringen rörande polisens uppgifter i 1 kap. 1 § 1 mom. i polislagen.

Paragrafens 2 punkt ändras dessutom så att ”avslöjande av brott” läggs till. Denna ändring är teknisk, eftersom det har ingått i polisens uppgifter att avslöja brott ända sedan ingången av 2014.

45 §. *Inskränkningar i rätten till insyn.* Enligt förslaget ska 1 mom. 5 punkten ändras så att rätten till insyn inte ska gälla uppgifter som erhållits vid utövande av befogenheterna enligt 4 kap. 3 § eller 5 eller 5 a kap. i polislagen, befogenheterna enligt 10 kap. i tvångsmedelslagen eller befogenheterna enligt lagen om civil underrättelseinhämtning avseende datatrafik. Dessutom stryks hänvisningen till den upphävda lagen om dataskydd vid elektronisk kommunikation.

Med laglighetskontroll av information avses inte en kontroll av att den ursprungliga inhämtningen varit laglig och ändamålsenlig, utan av att behandlingen av informationen varit lagenlig. Lagenligheten i behandlingen av de registrerade uppgifterna kontrolleras av dataombudsmannen på begäran på det sätt som anges i 2 mom.

1.5 Förundersökningslag

2 kap. **Vilka som deltar i förundersökning**

1 §. *Myndigheterna vid förundersökning.* Paragrafens 1 mom. ändras så att skyddspolisen inte ska vara en förundersökningsmyndighet. Enligt momentet görs förundersökning av någon annan polis än skyddspolisen.

Begränsningen av skyddspolisens befogenheter vid förundersökning sammanhänger med att skyddspolisens ges ökade befogenheter inom underrättelseverksamheten. För närvarande får skyddspolisen för att förhindra och avslöja brott använda de hemliga metoder för inhämtande av information som avses i 5 kap. i polislagen och för att utreda brott de hemliga tvångsmedel som avses i 10 kap. i tvångsmedelslagen. I överensstämmelse med vad som sagts i den allmänna motiveringen för man för att trygga rättvisa rättegångar överväga att begränsa skyddspolisens uppgifter och befogenheter vad gäller förundersökning. En begränsning av befogenheterna vid förundersökning förhindrar likväl inte att skyddspolisen deltar i en förundersökning som utförs av en förundersökningsmyndighet i egenskap av expertmyndighet.

1.6 Strafflag

12 kap. **Om landsförräderibrott**

12 §. *Begränsningsbestämmelse*. I paragrafen föreskrivs det att användning av metoder för underrättelseinhämtning enligt 5 a kap. i polislagen (872/2011), lagen om civil underrättelseinhämtning avseende datatrafik (/) eller lagen om militär underrättelseverksamhet (/) inte ska anses som brott enligt 12 kap. i strafflagen. Med detta avses att en tjänsteman som använder en metod för underrättelseinhämtning och en person som är föremål för underrättelseinhämtning när de verkar i enlighet med underrättelselagstiftningen inte gör sig skyldiga till en handling som avses i 12 kap. Vid en täckoperation kan tjänstemän till exempel hamna i situationer där deras förfaranden uppfyller en brottsbeskrivning och där de utan den föreslagna begränsningsbestämmelsen skulle medföra straffrättsligt ansvar. Det får inte bli beroende av

rättspraxis hur en täckoperation eller annan underrättelseverksamhet som sker i enlighet med lagstiftningen om underrättelseverksamhet förhåller sig till 12 kap. i strafflagen.

1.7 Tvångsmedelslag

2 kap. **Gripande, anhållande och häktning**

9 §. *Anhållningsberättigade tjänstemän.* Paragrafens 1 mom. 1 punkt ska enligt förslaget ändras så att chefen för skyddspolisen, biträdande chef som förordnats att sköta förundersökningsuppgifter, avdelningschef som förordnats att sköta förundersökningsuppgifter och överinspektör och inspektör som förordnats att sköta förundersökningsuppgifter stryks. Dessa ska inte längre vara anhållningsberättigade tjänstemän. Ändringen sammanhänger med den ändring i förundersökningslagen som föreslagits ovan.

10 kap. **Hemliga tvångsmedel**

3 §. *Teleavlyssning och dess förutsättningar.* Enligt förslaget ska definitionen av teleavlyssning i första meningen i 1 mom. ändras, eftersom det i den gällande definitionen ingår en hänvisning till kommunikationsmarknadslagen som upphävts.

Enligt den föreslagna definitionen ska med teleavlyssning avses att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett sådant allmänt kommunikationsnät eller ett sådant därtill anslutet kommunikationsnät som avses i 3 § 43 punkten i lagen om tjänster inom elektronisk kommunikation avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 8 §. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas göra sig skyldig till ett brott som avses i 2 mom.

Syftet med ändringen är inte att i sak ändra definitionen av teleavlyssning eller dess tillämpningsområde, utan ändringen är teknisk

6 §. *Teleövervakning och dess förutsättningar.* I paragrafens 1 mom. föreslås det att definitionen av teleövervakning justeras därför att det i definitionen i gällande lag hänvisas till den upphävda lagen om dataskydd vid elektronisk kommunikation samt via en hänvisningskedja till den upphävda kommunikationsmarknadslagen som nämns i definitionsbestämmelsen (3 §).

Enligt den föreslagna definitionen ska med teleövervakning avses att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät som avses i 3 § eller som har mottagits till en sådan adress eller utrustning samt att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att användningen av adressen eller utrustningen tillfälligt förhindras. Med identifieringsuppgifter avses uppgifter om ett meddelande vilka kan förknippas med en sådan användare som avses i 3 § 7 punkten i informationssamhällsbalken eller med en sådan abonnent som avses i 30 punkten i den paragrafen och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.

Syftet med ändringen är inte att i sak ändra definitionen av teleövervakning eller dess tillämpningsområde, utan ändringen är teknisk

39 §. *Användning av informationskällor och förutsättningar för styrd användning av informationskällor* Med användning av informationskällor ska enligt paragrafen avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av i 1 kap. 1 § av-

sedda uppgifter av personer som inte hör till polisen eller till någon annan myndighet (informationskälla).

I gällande lag kan informationskällor endast vara personer som inte hör till polisen eller till någon annan förundersökningsmyndighet. I praktiken har det i viss mån varit föremål för tolkning om andra tjänstemän än sådana som är anställda hos en förundersökningsmyndighet ska registreras som informationskälla. Därför föreslås det att definitionen preciseras på det sätt som nämnts ovan, det vill säga en informationskälla är en person som inte hör till polisen eller till någon annan myndighet.

1.8 Lag om offentlighet vid rättegång i allmänna domstolar

5 §. *Tidpunkten för när de grundläggande uppgifterna om en rättegång blir offentliga.* Det föreslås att 1 mom. ändras så att det till momentet fogas en hänvisning till ett nytt 3 mom. Detta behövs med anledning av det nya 3 mom. som föreslås.

I det 5 a kap som enligt förslaget ska fogas till polislagen (872/2011) och i 4 kap. i lagen om militär underrättelseverksamhet föreskrivs det bland annat om teleavlyssning och teleövervakning och annat motsvarande inhämtande av information. I lagen om civil underrättelseinhämtning avseende datatrafik och i 5 kap. i lagen om militär underrättelseverksamhet föreskrivs det å sin sida om underrättelseinhämtning som avser datatrafik. Med beaktande av att det till exempel för användning av dessa metoder för underrättelseinhämtning krävs tillstånd av en domstol, kommer uppgifter om behandlingen av ett sådant ärende lätt ut i offentligheten innan målen för den civila eller militära underrättelseinhämtningen uppnås, om det inte föreskrivs annorlunda om tidpunkten för offentliggörande av grundläggande uppgifter om rättegången än i 4 § i lagen om offentlighet vid rättegång i allmänna domstolar. Enligt den bestämmelsen är uppgifterna om den domstol som behandlar ärendet, ärendets exakta art, processens gång samt den muntliga förhandlingens tid och plats såväl som de uppgifter som är nödvändiga för specificering av parter genast offentliga.

Av dessa orsaker föreslås det att 5 § 2 mom. i lagen om offentlighet vid rättegång i allmänna domstolar kompletteras så att där nämns i fråga om såväl de hemliga metoder för inhämtande av information som avses i 10 kap. i tvångsmedelslagen, 5 kap. i polislagen och lagen om brottsbekämpning inom Tullen som de metoder för underrättelseinhämtning som avses i 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik och lagen om militär underrättelseverksamhet att de grundläggande uppgifterna ska bli offentliga först när den som blivit föremål för användningen av metoden för underrättelseinhämtning senast måste underrättas om detta. I 5 a kap. 46 § i polislagen, 20 § i lagen om civil underrättelseinhämtning avseende datatrafik och 87 § i lagen om militär underrättelseverksamhet föreskrivs det om att underrätta föremålet för underrättelseinhämtningen. Om underrättelsen får lämnas ogjord med stöd av ett domstolsbeslut enligt 5 a kap. 46 § 2 mom. i polislagen och 87 § 4 mom. i lagen om militär underrättelseverksamhet, blir inte heller de grundläggande uppgifterna om rättegången offentliga.

Momentet justeras också så att om personen i fråga underrättas om användningen av en metod för underrättelseinhämtning senare när personens identitet blivit känd, blir de grundläggande uppgifterna offentliga när domstolen informeras om underrättelsen. Bestämmelsen enligt vilken domstolen har en prövningsrätt som innebär att den får besluta att de grundläggande uppgifterna ska bli offentliga tidigare men inte att det ska ske senare, ska utsträckas till att gälla även användningen av metoder för underrättelseinhämtning.

I tullagen (1466/1994) har 20 f § upphävts genom lagen om ändring av tullagen 624/2015. När det gäller Tullen finns bestämmelser om hemliga metoder för inhämtande av information för

närvarande i lagen om brottsbekämpning inom Tullen. Hänvisningen i momentet till 20 f § i tullagen byts därför ut mot en hänvisning till 3 kap. i lagen om brottsbekämpning inom Tullen.

Dessutom föreslås det i 5 § ett nytt 3 mom., vars syfte är att ändra paragrafen så att man vid domstolsbehandlingen av ett i 15 § i lagen om övervakning av underrättelseverksamheten avsett interimistiskt förordnande av underrättelseombudsmannen som gäller avbrott eller upphörande av användningen av en metod för underrättelseinhämtning ska tillämpa samma offentlighetsregler som när det gäller tillståndsärenden som gäller metoder för underrättelseinhämtning.

12 §. *En parts rätt att ta del av en handling.* Det föreslås att 2 mom. 3 punkten i paragrafen kompletteras så att en part inte har rätt att få information om rättegångshandlingar i ett ärende som gäller en metod för underrättelseinhämtning som avses i 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik eller lagen om militär underrättelseverksamhet och där den person som är föremål underrättelseinhämtningen inte behöver höras vid behandlingen av yrkandet. Dessa ärenden ska likt de ärenden om metoder för hemligt inhämtande av information som nämns i momentet ställas utanför parternas rätt till information tills de blir offentliga enligt 16 § 4 mom. i lagen om offentlighet vid rättegång i allmänna domstolar.

Det föreslås en ny 3 a punkt i momentet, enligt vilken det i ett ärende som gäller ett i 15 § i lagen om övervakning av underrättelseverksamheten (/) avsett interimistiskt förordnande av underrättelseombudsmannen i fråga om tidpunkten för offentliggörande ska tillämpas vad som föreskrivs i 2 mom. När det gäller motiven till ändringen av bestämmelsen hänvisas det till motiven för 5 § 3 mom.

16 §. *Offentligheten i tvångsmedelsärenden.* I den paragraf som gäller offentligheten i tvångsmedelsärenden ska det enligt förslaget i fråga om en del tvångsmedelsärenden införas särskilda bestämmelser om rättegångshandlingarnas och domstolsavgörandets offentlighet. De särskilda bestämmelser som gäller tvångsmedelsärenden har samlats i denna paragraf, eftersom de centrala tvångsmedlen ska behandlas i normal ordning vid muntlig förhandling. Specialbestämmelsen om så kallad diarieoffentlighet ska å sin sida placeras i det ändrade 5 § 2 mom., eftersom bestämmelserna om diarieoffentlighet i allmänhet ska tillämpas i ett annat sammanhang än övriga bestämmelser om rättegångars offentlighet.

När en metod för underrättelseinhämtning används är det fråga om ärenden som avgörs utan att den person som är föremål för användningen hörs. Därför är det nödvändigt att inte heller allmänheten har tillträde till eventuella sammanträden där ärendet behandlas eller ges uppgifter om de avgöranden som gjorts vid sammanträdet och de handlingar som ingår i dem. Annars förfelas syftet med användningen av metoden. Därför föreslås det att 4 punkten i momentet ändras så att även ett ärende som gäller en metod för underrättelseinhämtning som avses i 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik eller lagen om militär underrättelseverksamhet och där den person som är föremål underrättelseinhämtningen inte behöver höras vid behandlingen av yrkandet ska handläggas och avgörandet avkunnas utan att allmänheten är närvarande. Den rättegångshandling som innehåller avgörandet samt övriga rättegångshandlingar i ärendet blir offentliga när den som är föremål för metoden för underrättelseinhämtning senast ska underrättas om att metoden använts.

I momentet ska det ytterligare föreskrivas att om personen i fråga underrättas om användningen av en metod för underrättelseinhämtning senare när personens identitet blivit känd, blir rättegångshandlingarna offentliga när domstolen informeras om underrättelsen. Domstolens rätt att tidigarelägga den tidpunkt då de grundläggande uppgifterna om rättegången blir offentliga

ska förutom ärenden som rör hemligt inhämtande av information även gälla ärenden som rör användningen av metoder för hemlig underrättelseinhämtning.

Av samma orsak som nämndes i samband med motiveringarna till 5 § ovan ska det i stället för 20 f § i tullagen hänvisas till 3 kap. i lagen om brottsbekämpning inom Tullen.

Det föreslås ett nytt 5 mom. i paragrafen, enligt vilket ett ärende som gäller ett i 15 § i lagen om övervakning av underrättelseverksamheten (/) avsett interimistiskt förordnande av underrättelseombudsmannen ska handläggas och avgörandet avkunnas utan att allmänheten är närvarande. I fråga om tidpunkten för när den rättegångshandling som innehåller avgörandet samt övriga rättegångshandlingar blir offentliga tillämpas 4 mom.

Med stöd av lagens 9 § är rättegångshandlingar sekretessbelagda till den del de innehåller uppgifter vilkas offentlighet sannolikt skulle äventyra statens yttre säkerhet eller medföra betydande skada eller olägenhet för Finlands internationella förbindelser eller förutsättningar att delta i det internationella samarbetet. Även efter den tidpunkt som anges i 4 mom. kan en rättegångshandling vara sekretessbelagd med stöd av 9 eller 10 § och ett domstolsavgörande med stöd av 24 §.

2 Ikraftträdande

Ett viktigt syfte med propositionen är att göra det möjligt att utveckla underrättelseinhämtningen så att den motsvarar den förändrade omvärlden och så att det kan produceras tillförlitlig och rättidig underrättelseinformation om hot mot Finlands säkerhetspolitiska miljö till stöd för det utrikes- och säkerhetspolitiska beslutsfattandet. Enligt säkerhetsmyndigheternas bedömning strävar främmande makter hela tiden efter att rikta ett avancerat cyberspionage mot Finlands statsförvaltning och mot finländska företag.

Samtidigt som den säkerhetspolitiska miljön förändrats och krisernas tidsspann blivit kortare har det skett en digitalisering av kommunikationssystemen. Denna utveckling har lett till att den civila underrättelseinhämtningen har sämre möjligheter att producera rättidig underrättelseinformation. Inte bara den externa utan även den interna säkerhetspolitiska miljön har blivit alltmer utmanande och det har blivit svårare att förutse olika situationer.

I den allmänna motiveringen konstateras det att Finlands befogenheter att inhämta information är otidsenliga i internationell jämförelse med den övriga utvecklingen i Europa. För att uppnå europeisk medelnivå krävs det en långsiktig utveckling av underrättelsesystemen och underrättelsemetoderna. Detta utvecklingsarbete kan inte inledas förrän de föreslagna nya behörighetsbestämmelserna träder i kraft. Finlands förmåga till underrättelseinhämtning försvagas därför hela tiden i förhållande till andra stater så länge den föreslagna regleringen inte är i kraft.

För att det ska vara möjligt att upprätthålla Finlands fortlöpande förmåga att skydda den nationella säkerheten är det av kritisk betydelse att alla de metoder för underrättelseinhämtning som föreslås i propositionen kan användas av skyddspolisen så snart som möjligt. Med hjälp av metoderna för underrättelseinhämtning kan skyddspolisen upprätthålla den förmåga till underrättelseinhämtning som behövs vid uppföljningen av förändringar i omvärlden.

Genom den information som får inhämtas med stöd av de föreslagna befogenheterna kan man stödja terrorismbekämpningen och svara mot allvarliga hot som riktar sig mot Finland. De befogenheter som ingår i lagen om civil underrättelseinhämtning avseende datatrafik ska också användas till att stödja andra myndigheter. Om befogenheterna fördröjs kommer därför också andra myndigheters förmåga att sköta sina lagstadgade uppgifter att blir sämre.

Behovet av ett brådskande förfarande beror inte på enstaka händelser som förekommit i offentligheten utan behovet grundar sig på en helhetsbedömning av utvecklingen i Finlands säkerhetspolitiska miljö.

Förändringen i omvärlden har varit snabb och den fortgår alltjämt. Därför bör de bestämmelser som föreslås för att möjliggöra den civila underrättelseinhämtningen, som är av kritisk betydelse för Finlands nationella säkerhet, i sin helhet träda i kraft så snart som möjligt. Då kan man svara mot de snabba förändringarna i Finlands säkerhetspolitiska miljö och möjliggöra en tillräckligt effektiv informationsinhämtning för att skydda Finlands nationella säkerhet.

Av de skäl som angetts ovan föreslås lagarna träda i kraft så snart som möjligt.

I 5 a kap. i det förslag till ändring av polislagen som ingår i propositionen föreskrivs det om teleavlyssning och inhämtande av information i stället för teleavlyssning (5 §), teleövervakning (6 §), teknisk avlyssning (10 §), kopiering av försändelser (28 §) och underrättelseinhämtning som avser datatrafik, som det också föreskrivs om i den helt nya lagen om civil underrättelseinhämtning avseende datatrafik. Dessa frågor anknyter till justitieministeriets förslag om att justera en del bestämmelser i grundlagen. Justitieministeriets förslag till ändring av 10 § 3 mom. i grundlagen ska behandlas i den ordning som föreskrivs i 73 § i grundlagen.

Om förslaget till ändring av grundlagen behandlas i den lagstiftningsordning som anges i 73 § 1 mom. i grundlagen, kan de ovan nämnda bestämmelserna i 5 a kap. i polislagen och i lagen om civil underrättelseinhämtning avseende datatrafik eventuellt träda i kraft den 1 januari 2020.

Om förslagen till ändring av grundlagen däremot behandlas i den lagstiftningsordning som anges i 73 § 2 mom. i grundlagen, kan 5 a kap. i polislagen samt lagen om civil underrättelseinhämtning avseende datatrafik träda i kraft 2018 eller vid ingången av 2019.

Om förslaget till ändring av grundlagen behandlas i den lagstiftningsordning som anges i 73 § 1 mom. i grundlagen, föreslås det dock att alla andra bestämmelser än de som kräver en grundlagsändring ska träda i kraft så snart som möjligt 2018 eller vid ingången av 2019.

Propositionen har dessutom ett nära samband med de regeringspropositioner som beretts vid försvarsministeriet och justitieministeriet och som gäller en lag om militär underrättelseverksamhet och en lag om övervakning av underrättelseverksamheten. Därför bör alla dessa lagar träda i kraft samtidigt.

3 Förhållande till grundlagen samt lagstiftningsordning

3.1 Inledning

Propositionen har beröringspunkter särskilt med rättsstatsprincipen i 2 § 3 mom. i grundlagen och med skyddet för de grundläggande fri- och rättigheterna i 9, 10, 15 och 21 § i grundlagen. Genom de befogenheter som ingår i lagstiftningen om civil underrättelseinhämtning ingriper man i många fall i individens grundläggande fri- och rättigheter. Mest betydelsefulla från grundlagssynpunkt är de föreslagna bestämmelser där myndigheterna får nya befogenheter gentemot individen eller genom vilka individens rättigheter och handlingsfrihet begränsas på annat sätt.

Även om man genom användning av metoder för underrättelseinhämtning inkräktar på vissa grundläggande rättigheter, såsom skyddet för privatlivet, strävar man vid tillämpningen av lagen om civil underrättelseinhämtning avseende datatrafik likväl efter att skydda övriga grund-

läggande fri- och rättigheter, såsom statens självbestämmanderätt. Människornas kollektiva säkerhet liksom samhällets vitala funktioner och ett organiserat samhällsliv är så viktiga intressen att försvara att det för en lagstiftning om underrättelseverksamhet finns ett tungt vägande samhälleligt behov och en godtagbar grund med beaktande av systemet av grundläggande fri- och rättigheter.

Vid civil underrättelseinhämtning är det enligt förslaget tillåtet att inhämta information endast om objekt som ingår i en uttömmande förteckning som ingår i lagen. Det föreslås att det ska lagstiftas om dem så specifikt som möjligt med beaktande av underrättelseverksamhetens särskilda karaktär. Bestämmelserna om metoderna för underrättelseinhämtning föreslås bli så precisa och exakt avgränsade som möjligt.

Eftersom underrättelseverksamhet kan anförtros endast en myndighet som sköter den nationella säkerheten, föreslås det att skyddspolisen ensam ska sköta den civila underrättelseinhämtningen.

Lagförslagen granskas dessutom med hänsyn till de allmänna villkoren för att begränsa grundläggande fri- och rättigheter, egendomsskyddet och rättssäkerheten samt 124 § i grundlagen (Överföring av förvaltningsuppgifter på andra än myndigheter).

3.2 Granskning av befogenhetsbestämmelserna med hänsyn till bestämmelserna om grundläggande fri- och rättigheter

Skydd för privatlivet

I 10 § i grundlagen föreskrivs det om skydd för privatlivet. En av de principer som ligger till grund för bestämmelsen är att individen har rätt att leva sitt liv utan att myndigheter eller andra utomstående aktörer på ett godtyckligt sätt och utan giltig orsak ingriper i privatlivet. Paragrafen ger var och en rätt till konfidentiell kommunikation utan att utomstående får information om innehållet i konfidentiella meddelanden som han eller hon skickar eller tar emot. Detta innebär till exempel skydd mot att brev eller andra slutna meddelanden öppnas eller förstörs samt mot avlyssning och upptagning av samtal. Lagstiftningen skyddar inte endast meddelandets avsändare, utan det handlar om en grundläggande rättighet som båda parterna i kommunikationen ska åtnjuta. Förutom innehållet i ett meddelande skyddar grundlagen också identifikationsuppgifterna för avsändaren och mottagaren samt övrig information som kan ha betydelse med hänsyn till bevarandet av sekretessen.

Hemfrid

Metoder för underrättelseinhämtning som är betydelsefulla med hänsyn till 10 § i grundlagen är systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, täckoperationer, bevisprovokation genom köp och platsspecifik underrättelseinhämtning. Ingen av de metoder för underrättelseinhämtning som nämns ovan får riktas mot ett utrymme som används för stadigvarande boende, med undantag för täckoperationer och bevisprovokation genom köp som ska vara tillåtet i bostäder under aktiv medverkan av den som använder bostaden. Den grundlagstryggade hemfriden omfattar i princip alla slag av utrymmen som används för boende av permanent natur. Genom de föreslagna metoderna för underrättelseinhämtning gör man alltså inte intrång i kärnområdet för det hemfridsskydd som avses i grundlagen (GrUU 43/2010 rd, s. 2, GrUU 40/2010 rd, s. 4, GrUU 18/2010 rd, s. 7, GrUU 6/2010 rd, s. 4, GrUU 8/2006 rd, s. 2, GrUU 39/2005 rd, s. 2, GrUU 16/2004 rd, s. 5, GrUU 69/2002 rd, s. 2, GrUU 48/2001 rd, s. 2, GrUU 46/2001 rd, s. 3–4). Principen är att de metoder för underrättelseinhämtning som nämns här inte heller får riktas mot bostäder i utlandet. Att utreda användningsområdet för en bostad kan likväl visa sig vara omöjligt eller orimligt svårt

särskilt i mindre utvecklade länder. De metoder för underrättelseinhämtning som nämnts ovan kan därför inte anses vara problematiska med hänsyn till hemfriden som tryggas i 10 § 1 mom. i grundlagen.

Skydd för personuppgifter

Enligt 10 § 1 mom. i grundlagen ska närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Enligt grundlagsutskottets praxis begränsas lagstiftarens handlingsutrymme både av den här bestämmelsen och av att skyddet för personuppgifter delvis ingår i samma moment som skyddet för privatlivet (se t.ex. GrUU 71/2014 rd, s. 2). Grundlagsutskottet har av hävd ansett att lagstiftaren ska trygga skyddet för personuppgifter på ett sätt som är godtagbart med avseende på de grundläggande fri- och rättigheterna överlag (se t.ex. GrUU 18/2012 rd, s. 2 och GrUU 71/2012, s. 2). Vid bedömningen av den typ av registerbestämmelser som nu föreslås har grundlagsutskottet normalt fäst uppmärksamhet särskilt vid att om syftena för registreringen, innehållet i de registrerade personuppgifterna, de tillåtna användningsområdena för uppgifterna, möjligheterna till överlåtelse av personuppgifter och i synnerhet utlämnande genom teknisk anslutning, uppgifternas förvaringstid och den registrerades rättsskydd bör föreskrivas i lagbestämmelser som ska vara heltäckande och detaljerade (se t.ex. GrUU 12/2002 rd, s. 5, 19/2012 rd, s. 2 och GrUU 71/2014 rd, s. 2).

Inom den civila underrättelseinhämtningen hanteras också personuppgifter. I den revidering av lagen om behandling av personuppgifter i polisens verksamhet som är under beredning föreslås det att behandling av personuppgifter inom den civila underrättelseinhämtningen ska regleras i den föreslagna lagen och att bestämmelser om skyddspolisens behandling av personuppgifter ska ingå i den. I den propositionen beaktas de ändringsbehov som följer av Europeiska unionens dataskyddsförordning och direktivet om dataskydd i brottmål.

Avsikten är att regeringens proposition till riksdagen med förslag till lag om behandling av personuppgifter i polisens verksamhet, lag om genomförande av direktivet om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och till vissa lagar som har samband med dem ska lämnas till riksdagen så att den behandlas i riksdagen samtidigt med den regeringsproposition som gäller lagstiftningen om civil underrättelseinhämtning.

I lagen om behandling av personuppgifter i polisens verksamhet ska det på ett heltäckande sätt och i detalj föreskrivas om behandling av personuppgifter som gäller civil underrättelseinhämtning, deras användningsändamål och datainnehåll, utlämnande av personuppgifter till en annan stat och till internationella organisationer, skyddspolisens rätt att få personuppgifter för skötseln av sina uppgifter och om utplånande av personuppgifter ur skyddspolisens register.

Konfidentiella meddelanden

Teleavlyssning och inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, kopiering av försändelser och underrättelseinhämtning som avser datatrafik ska ses som betydande ingrepp i hemligheten i fråga om förtroliga meddelanden, som tryggas i 10 § 2 mom. i grundlagen, bortsett från situationer där det är fråga om kommunikation som en militärorganisation eller en annan myndighetsorganisation i en främmande stat bedriver. Även om teleövervakning tidigare har setts som ett mindre ingrepp i skyddet för konfidentiell kommunikation, kan identifieringsuppgifter som ansluter sig till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är (GrUU 18/2014 rd, s. 6). Vid en kon-

stitutionell granskning av underrättelseinhämtning som avser datatrafik bör det beaktas att redan sådan åtkomst till information som gör det möjligt att samla den innebär en kränkning av skyddet för privatlivet (Klass mot Saksatyskland, Liberty m.fl. mot Förenade kungariket).

Det är under alla omständigheter klart att det inte med stöd av 10 § 3 mom. i grundlagen är möjligt att lagstifta om sådana begränsningar i sekretessen i frågas om meddelanden som inte syftar till att förhindra brott utan vars syfte i är att i stället på ett allmännare plan inhämta information om allvarliga hot som är nödvändig med hänsyn till den nationella säkerheten. Följaktligen är det möjligt att i vanlig lagstiftningsordning lagstifta om inhämtande av information genom teleavlyssning och inhämtande av information i stället för teleavlyssning, teknisk avlyssning, kopiering av försändelser och metoder för underrättelseinhämtning som avser datatrafik för att värna den nationella säkerheten bara med stöd av en ny begränsningsgrund för inhämtande av information som enligt justitieministeriets förslag ska infogas i 10 § 4 mom. i grundlagen och under förutsättning att de allmänna villkoren för begränsning av de grundläggande friheterna och rättigheterna uppfylls. Den nya begränsningsgrund rörande inhämtande av information som ska infogas i 10 § 4 mom. i grundlagen gör det inte möjligt att lagstifta om en allmän övervakning som inte är inriktad på specifika föremål utan gäller all datatrafik.

I lagstiftningen om inhämtande av basstationsuppgifter, systematisk observation, förtäckt informationsinhämtning, optisk observation, teknisk spårning, täckoperationer, bevisprovokation genom köp och platsspecifik underrättelseinhämtning har de allmänna begränsningsvillkoren enligt avsnitt 3.2.3 nedan beaktats. Därför och med beaktande av att metoderna i fråga i rätt obetydlig grad kränker sekretessen i fråga om konfidentiella meddelanden eller deras identifikationsuppgifter, ska de anses oproblematiska med hänsyn till 10 § 2 mom. i grundlagen.

Rörelsefrihet

I 9 § i grundlagen föreskrivs det om rörelsefrihet. Enligt paragrafen har finska medborgare samt utlänningar som lagligen vistas i landet rätt att röra sig fritt inom landet och att där välja bostadsort. Inskränkningar i rörelsefriheten ska grunda sig på lag. Vid en bedömning av om en begränsning kan tillåtas ska avseende fästas vid artikel 2 i 4 tilläggsprotokollet till europeiska konventionen för mänskliga rättigheter. Enligt stycke 3 ska begränsningar av rörelsefriheten vara lagenliga och nödvändiga i ett demokratiskt samhälle (RP 309/1993 rd). De metoder för underrättelseinhämtning som är betydelsefulla med hänsyn till 9 § i grundlagen är inhämtande av basstationsuppgifter, systematiska observation, optisk observation och teknisk spårning (GrUU 36/2002 rd, s. 5). Metoderna i fråga innebär en rätt obetydlig intervention i rörelsefriheten i jämförelse med nödvändigheten hos den begränsningsgrund som den nationella säkerheten i ett demokratiskt samhälle utgör. Följaktligen bedöms bestämmelserna om de metoder för underrättelseinhämtning som nämnts här inte vara problematiska med hänsyn till rörelsefriheten.

Förutsättningar för begränsning av grundläggande fri- och rättigheter

Nödvändighet

En begränsning av hemligheten i fråga om förtroliga meddelanden ska enligt det föreslagna 4 mom. i 10 § i grundlagen vara nödvändig. Detta villkor följer också av de allmänna förutsättningarna för begränsning av grundläggande fri- och rättigheter.

När man bedömer nödvändigheten hos bestämmelser i ett lagförslag ska man beakta att en metod för underrättelseinhämtning som ingriper i skyddet för sekretessen i fråga om konfidentiella meddelanden får användas för inhämtande av information om en verksamhet som är föremål för civil underrättelseinhämtning endast om verksamheten allvarligt hotar den nationella

säkerheten (5 a kap. 4 § i polislagen). Föremålen för civil underrättelseinhämtning anges i lagen på ett uttömmande sätt, vilket motsvarar kraven i Europadomstolens rättspraxis. Att det i lagen till exempel enbart nämns att hemliga befogenheter får användas för att skydda den nationella säkerheten, är inte tillräckligt för att uppfylla kravet på förutsebarhet (Zakharov mot Ryssland). Man kan inte heller kräva att den nationella lagstiftningen på ett exakt och uttömmande sätt ska ange alla de situationer där myndigheterna får använda hemliga befogenheter. En bestämmelse i lag om att terrorhot är en grund för utövande av hemliga befogenheter kan till exempel anses uppfylla det krav på förutsebarhet som ställs i Europakonventionen (Szabó & Vissy mot Ungern). Genom metoder för civil underrättelseinhämtning får man inhämta information om terrorism, utländsk underrättelseverksamhet, planering, tillverkning och spridning av massförstörelsevapen och produkter med dubbel användning, verksamhet som hotar den demokratiska samhällsordningen, verksamhet som hotar ett stort antal människors liv eller hälsa eller samhällets vitala funktioner, en främmande stats verksamhet som kan orsaka skada för Finlands internationella relationer, ekonomiska intressen eller andra viktiga intressen, en kris som hotar internationell fred och säkerhet, verksamhet som hotar säkerheten vid internationella krishanteringsinsatser, verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och deltar i annan internationell verksamhet samt internationell organiserad brottslighet som hotar samhällsordningen (polislagens 5 a kap. 3 §).

I 5 a kap. 3 § i polislagen som behandlar föremålen för civil underrättelseinhämtning specificeras och konkretiseras således det föreslagna nya 4 mom. i 10 § i grundlagen, enligt vilket det med verksamhet som allvarligt hotar den nationella säkerheten avses verksamhet som hotar den demokratiska stats- och samhällsordningen, samhällets grundläggande funktioner, ett stort antal människors liv eller hälsa eller internationell fred och säkerhet. Eftersom varje punkt i den först nämnda bestämmelsen kan härledas ur ett eller flera av de skyddsintressen som omfattas av begreppet nationell säkerhet, bedöms det att paragrafen uppfyller kraven på nödvändighet och förutsägbarhet, vars betydelse här accentueras.

Exakthet och noggrann avgränsning

De allmänna förutsättningarna för användning av metoder för underrättelseinhämtning ska anges i 5 a kap. 4 § i polislagen (Amann mot Schweiz, Kopp mot Tyskland, Kruslin mot Frankrike, Huvig mot Frankrike). Ett allmänt villkor för samtliga metoder för underrättelseinhämtning är att metoden av grundad anledning kan antas ge information om en sådan verksamhet som allvarligt hotar den nationella säkerheten och som är objekt för underrättelseinhämtningen. Det är fråga om så kallad grundad resultatförväntning. Eftersom teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, systematisk observation, teknisk avlyssning, optisk observation, teknisk spårning av en person, teknisk observation av utrustning, styrd användning av informationskällor och platsspecifik underrättelseinhämtning kan innebära betydande ingrepp i en privatpersons skyddade rättsobjekt, är en förutsättning för dessa metoders del också att användningen av dem med fog kan antas vara av synnerligen stor betydelse för att få av information om verksamhet som allvarligt hotar den nationella säkerheten. För användning av täckoperationer och bevisprovokation genom köp krävs det enligt förslaget dessutom att metoden är nödvändig för att få information om verksamhet som allvarligt hotar den nationella säkerheten.

Det föreskrivs också om särskilda förutsättningar för användningen av metoder för underrättelseinhämtning och dessa förutsättningar föreskrivs det om i 5 a kap. 4 § i polislagen (Amann mot Scheiz, Kopp mot Tyskland, Kruslin mot Frankrike, Huvig mot Frankrike). I lagstiftningen om metoderna för underrättelseinhämtning anges bland annat vilken information som ska ingå i ett yrkande och ett beslut om användning av metoden, liksom vem som beslutar om underrättelseinhämtningen samt giltighetstiden för det tillstånd, beslut eller förordnande som avser underrättelseinhämtningen.

Acceptabilitet och proportionalitet

Vid användning av metoder för underrättelseinhämtning ska man respektera de grundläggande fri- och rättigheterna, de mänskliga rättigheterna, proportionalitetsprincipen och principen om ändamålsbundenhet. Kravet att de grundläggande fri- och rättigheterna och de mänskliga rättigheterna ska respekteras innebär bland annat att skyddspolisen när den använder sina befogenheter för underrättelseinhämtning bland de motiverbara metoderna för underrättelseinhämtning ska välja den som bäst tillgodoser dessa rättigheter. Proportionalitetsprincipen innebär att man måste bedöma om användningen av en metod för underrättelseinhämtning är försvarbar med beaktande av hur viktigt och brådskande underrättelseuppdraget är, målet för uppdraget och övriga omständigheter som har betydelse vid en helhetsbedömning av situationen. Såväl Europadomstolen som EU-domstolen har i sin rättspraxis understrukit vikten av att proportionalitetsprincipen iakttas särskilt i samband med underrättelseinhämtning som avser datatrafik (t.ex. Zakharov mot Ryssland, Weber och Saravia mot Tyskland, Digital Rights Ireland). Det krävs därför att underrättelseinhämtning som avser datatrafik är en metod som används i sista hand, det vill säga att inhämtande av information på något annat sätt är omöjligt eller orimligt svårt. Av principen om minsta olägenhet följer att skyddspolisen genom sina åtgärder inte får ingripa i någons rättigheter i större utsträckning eller orsaka någon större skada eller olägenhet än vad som är nödvändigt för att utföra underrättelseuppdraget. Det är klart att skyddspolisen enligt principen om ändamålsbundenhet får använda sina befogenheter för underrättelseinhämtning endast för föreskrivna ändamål.

Rättssäkerhetsmekanism

Vid underrättelseverksamhet accentueras betydelsen av tillräckliga rättssäkerhetsmekanismer och effektiv övervakningen. Det är viktigt att underrättelsemyndigheten inte har obegränsad prövningsrätt när det gäller inriktningen av inhämtandet av information. Ett sätt att begränsa myndighetens prövningsrätt är att ålägga en domstol att besluta om användningen av de metoder för underrättelseinhämtning som ingriper mest i skyddet för de grundläggande fri- och rättigheterna (bl.a. Weber och Saravia mot Tyskland). Enligt förslaget krävs domstolstillstånd för teleavlyssning och inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, teknisk avlyssning, optisk observation, teknisk spårning, teknisk observation av utrustning, platsspecifik underrättelseinhämtning och underrättelseinhämtning som avser datatrafik. Tillståndet ska kunna beviljas för högst sex månader åt gången med undantag av teleavlyssning och inhämtande av information i stället för teleavlyssning som riktar sig mot en person. I sådana fall kan tillstånd enligt förslaget beviljas för högst tre månader åt gången.

Även de föreslagna bestämmelserna om förbud mot avlyssning och observation, kopieringsförbud och förbud mot underrättelseinhämtning, utplåning av underrättelseinformation och underrättelse om användning av metoder för underrättelseinhämtning bidrar till att trygga rättssäkerheten. Rätten att få underrättelse om att man har blivit föremål för underrättelseinhämtning är viktig för att personen över huvud taget ska kunna få sin sak prövad. Den som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning och teknisk observation samt underrättelseinhämtning som avser datatrafik ska utan dröjsmål underrättas om detta efter det att syftet med inhämtandet av information har nåtts. Underrättelse om användning av övriga metoder ska göras om förundersökning inleds i ärendet. Den föreslagna lagstiftningen ger envar som misstänker att den blivit föremål för en kränkning av skyddet för privatlivet möjlighet att få sin sak behandlad på behörigt sätt vid en domstol eller en annan myndighet enligt vad som föreskrivs i 21 § i grundlagen.

Partsoffentligheten är en viktig garanti för rättssäkerheten för den som blivit föremål för inhämtning av information. Användningen av metoder för underrättelseinhämtning omfattas av

partsoffentligheten från det att personen som blivit föremål för underrättelseinhämtningen underrättats om detta. Alla ärenden som gäller användning av metoder för underrättelseinhämtning omfattas av diarieoffentligheten, handlingsoffentligheten, offentligheten i fråga om avgöranden och partsoffentligheten.

För en effektiv övervakning av underrättelseverksamheten krävs det att övervarningsorganen har tillgång till allt material som samlats genom underrättelseverksamheten och rätt att granska information och handlingar. Därför gäller för metoderna för underrättelseinhämtning en skyldighet att utan dröjsmål protokollföra varje åtgärd. Om detta ska det föreskrivas närmare genom förordning på motsvarande sätt som det föreskrivs om protokollföring i statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information (122/2014).

Den externa laglighetskontrollen ska enligt förslaget vid sidan av de högsta laglighetsövervakarna skötas av en ny myndighet, underrättelseombudsmannen, som ska övervaka underrättelseinhämtningen i realtid. För att möjliggöra övervakning i realtid föreskrivs det enligt förslaget om en skyldighet att lämna underrättelseombudsmannen information om domstolens beslut om och tillstånd för användning av metoderna så snart som möjligt efter det att beslut om att lämna ut informationen fattats. Dessutom ska skyddspolisen så snart som möjligt underrätta underrättelseombudsmannen om ett beslut som inte hör till en domstols beslutsbehörighet och som gäller användning av en metod för underrättelseinhämtning, skydd av civil underrättelseinhämtning, yppandeförbud eller senareläggning av överföringen av information för brottsbekämpning.

Ombudsmannen ska ha omfattande rätt till information och rätt att få utredningar av myndigheter och andra aktörer som sköter offentliga förvaltningsuppgifter. Ombudsmannen ska enligt förslaget kunna göra inspektioner för att övervaka lagligheten i underrättelseverksamheten. Dessutom föreslås det att ombudsmannen ska ha tillgång till de utrymmen och datorsystem som är nödvändiga med hänsyn till övervakningen. Underrättelseombudsmannen kan dessutom förordna att användningen av en metod för underrättelseinhämtning ska avbrytas eller avslutas om han eller hon anser att den övervakade har förfarit lagstridigt i underrättelseverksamheten.

Inom inrikesförvaltningen ska övervakningen av underrättelseverksamheten skötas av skyddspolisen och inrikesministeriet. Den laglighetsövervakning som de bedriver ska förstärkas med nya personalresurser och effektiviseras genom att övervakningsinsatser börjar skötas i realtid Inrikesministeriet ska årligen till riksdagens justitieombudsman och underrättelseombudsmannen avge en berättelse om hur metoderna för underrättelseinhämtning och skyddet av dem har använts och övervakats.

Europadomstolen har sett det som viktigt att även medlemmar i folkrepresentationen deltar i övervakningen. Den parlamentariska övervakningen av underrättelseverksamheten ska enligt förslaget skötas av ett underrättelseutskott. Underrättelseutskottet ska fungera som en del av riksdagens utskottsväsende. För att sköta sitt övervakningsuppdrag ska utskottet utöver rätten till information ha rätt att få utredningar bland annat av underrättelseombudsmannen och andra myndigheter.

3.3 Övriga bestämmelser i grundlagsperspektiv

Yttrandefrihet och rättssäkerhet

I 5 a kap. 38 § i polislagen ska det enligt förslaget föreskrivas om ett yppandeförbud som gäller metoder för underrättelseinhämtning. Enligt bestämmelsen får en för uppdraget förordnad

polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för civil underrättelseinhämtning förbjuda en utomstående att röja sådana omständigheter om användningen av en metod för underrättelseinhämtning som denne fått kännedom om, om det är motiverat för att skydda metoden för underrättelseinhämtning. Det yppandeförbud som det är fråga om här kan inte anses begränsa den yttrandefrihet som ska tryggas enligt 12 § 1 mom. i grundlagen avsevärt med beaktande av de allmänna förutsättningarna för begränsning av en grundläggande frihet eller rättighet, särskilt kravet om exakthet och noggrann avgränsning samt acceptabilitetskravet. De krav som ställs för meddelande av yppandeförbud, såsom kravet på skriftlig form och specificering, anges detaljerat i lagen. För det första ska det vara nödvändigt att meddela ett yppandeförbud. För det andra ska en förutsättning för meddelande av ett yppandeförbud vara att den utomstående med anledning av sitt uppdrag eller sin ställning har bistått eller blivit ombedd att bistå vid användningen av en metod för underrättelseinhämtning (GrUU 28/2008 rd, s. 3, GrUU 67/2002 rd, s. 4, GrUU 28/1997 rd).

Bestämmelser om yppandeförbud är nödvändiga, eftersom en metod för underrättelseinhämtning kan bli omöjlig att använda eller så kan dess syfte äventyras om den person som är föremål för användningen av metoden får kännedom om detta via utomstående.

Ändring i ett beslut om yppandeförbud får inte sökas genom besvär. I beslutet ska besvärsförbudet och dess rättsliga grund nämnas. Den som meddelats yppandeförbud ska alltid ha rätt att underrätta underrättelseombudsmannen om yppandeförbudet. Dessutom ska den som meddelats yppandeförbud underrättas om möjligheten att anföra klagan hos hovrätten och om möjligheten att meddela underrättelseombudsmannen om yppandeförbudet. Rätten att anföra klagan kan tillsammans med underrättelseombudsmannens övervakning betraktas som en tillräcklig garanti för rättsskydd (Klass m.fl. mot Tyskland och Leander mot Sverige).

Eftersom skyddspolisen i praktiken aldrig kommer att ha behov eller ens rätt att offentligt informera om de omständigheter som gäller användningen av en metod för underrättelseinhämtning som omfattas av ett yppandeförbud, är meddelandet av yppandeförbud inte förknippat med motsvarande obalans som kan uppstå vid förundersökningar när undersökningsledaren informerar om omständigheter för vilka den misstänkte eller dennes biträde har meddelats yppandeförbud. Besvärsförbudet inkräktar inte på den rätt att söka ändring som tryggas i 21 § 2 mom. i grundlagen när man beaktar att meddelandet av förbudet föregås av ett tungt vägande skäl och att förbudet gäller omständigheter i samband med användningen av en metod för underrättelseinhämtning.

I 5 a kap. 39 § i polislagen ska det enligt förslaget föreskrivas om beslut om användning av metoder för underrättelseinhämtning i vissa fall. Enligt bestämmelsen fattas beslut om civil underrättelseinhämtning som genomförs och användning av metoder för underrättelseinhämtning någon annanstans än i Finland av chefen för skyddspolisen En finsk tjänsteman får naturligtvis inte heller i utlandet verka i strid med de universella fri- och rättigheterna eller de mänskliga rättigheterna. Därför och med beaktande av att en underrättelse till den som blivit föremål för användning av en metod för underrättelseinhämtning är en viktig garanti för rättssäkerheten, ska underrättelsen i vanliga fall göras också när verksamheten sker utomlands. Detta är emellertid inte alltid möjligt, och i en del situationer skulle underrättelsen kunna skada Finlands internationella relationer eller förutsättningar för att delta i internationellt samarbete och dessutom äventyra tjänstemannens liv eller hälsa. Underrättelsen skulle vara omöjlig till exempel i länder där förvaltningen kollapsat eller är bräcklig och där det inte finns myndighetsregister eller andra verktyg för att utreda identitet eller boningsort för den som blivit föremål för inhämtande av information. Av dessa orsaker och med beaktande att underrättelse om användning av en metod för underrättelseinhämtning enligt 47 § 2 mom. i vissa fall kan lämnas helt ogjord också i Finland, kan den paragraf som nämndes i inledningen av av-

snittet inte ses som problematisk med avseende på rättsskyddet enligt 21 § i grundlagen på grund av att underrättelsen är underkastad prövning

Egendomsskydd

I 5 a kap. 50 § i polislagen föreslås en bestämmelse om rätten att få information av privata sammanslutningar. Bestämmelsen ger skyddspolisen rätt att, trots den företags-, bank- och försäkringshemlighet som binder en sammanslutnings medlemmar, revisorer, verkställande direktör, styrelsemedlemmar eller arbetstagare, få uppgifter som kan antas vara behövliga vid utredningen av hot mot den nationella säkerheten. Bestämmelsen är betydelsefull för den som är föremål för en begäran om information för att denne inte vid överlämnandet av informationen till skyddspolisen ska göra sig skyldig till sekretessbrott eller en annan gärning som är straffbar enligt lag, utan tvärt om ska kunna lita att han eller hon handlar på ett sätt som är tillåtet i lagen. Bestämmelsen om rätten att få information av privata sammanslutningar är oproblematisk med hänsyn till såväl skyddet för privatlivet, som tryggas i 10 § 1 mom. i grundlagen, som egendomsskyddet som tryggas i 15 § 1 mom. med beaktande av det tvingande samhälleliga behov som ligger till grund för lagförslaget, förutsebarheten i den skyldighet att uppge vad man vet ur de personers synvinkel som skyldigheten gäller samt knytandet av den resultatförväntan som sammanhänger med begäran till precisa kriterier.

I 5 a kap. 51 § i polislagen ska det enligt förslaget infogas en bestämmelse om teleföretags skyldighet att biträda. I skyldigheten att biträda ingår att göra de kopplingar i ett telenät som behövs för teleavlyssning eller teleövervakning och att lämna polismyndigheten de uppgifter och redskap samt den personal som behövs för teleavlyssningen (RP 224/2010 rd s. 145). I 21 § i lagen om civil underrättelseinhämtning avseende datatrafik görs dataöverförare å sin sida skyldiga att lämna uppgifter. Det är fråga om dataöverförares skyldighet att lämna skyddspolisen de uppgifter som behövs för att inrikta underrättelseinhämtning som avser datatrafik. De skyldigheter som teleföretag och dataöverförare påförs får anses oproblematiska med hänsyn till egendomsskyddet som tryggas enligt 15 § 1 mom. i grundlagen, eftersom skyldigheterna finns inskrivna i tydliga bestämmelser och är skäliga för de aktuella företagen (GrUU 8/2002 rd och GrUU 61/2002 rd). Med tanke på skälighetsbedömningen ska det noteras att dataöverföraren inte är skyldig att lämna skyddspolisen någon information som är betydelselös med tanke på inriktandet av underrättelseinhämtningen och att dataöverförarens skyldighet att lämna uppgifter ska gälla endast sådana uppgifter som den redan innehar. Teleföretag och dataöverförare ska enligt förslaget ersättas för kostnader som fullgörandet av skyldigheten att biträda resp. fullgörandet av skyldigheten att lämna uppgifter orsakar dem.

Anförtroende av förvaltningsuppgifter till andra än myndigheter

I 5 a kap. 57 § i polislagen ska det enligt förslaget föreskrivas om internationellt samarbete. Enligt paragrafen ska skyddspolisen kunna samarbeta med och utföra gemensamma uppdrag tillsammans med utländska säkerhets- och underrättelsetjänster. Särskilda bestämmelser om att ge och begära internationellt bistånd finns i lagen om beslutsfattande om lämnande av och begäran om internationellt bistånd (418/2017). I paragrafen förutsätts det att en tjänsteman från en främmande stat som använder vissa metoder för underrättelseinhämtning i Finland iakttar förordnanden och anvisningar av en polisman vid skyddspolisen. Användningen av metoder för underrättelseinhämtningen kommer följaktligen alltid att styras och övervakas av en finsk tjänsteman. Dessutom har en tjänsteman från en främmande stat när han eller hon verkar i Finland straff- och skadeståndsrättsligt ansvar om något annat inte följer till exempel av dennes diplomatstatus. Tack vare dessa förfarandegarantier och ansvarsarrangemang bedöms den föreslagna paragrafen inte vara problematisk med hänsyn till den bestämmelse i 124 § i grundlagen enligt vilken uppgifter som innebär betydande utövning av offentlig makt får ges endast myndigheter.

3.4 Bedömning av lagstiftningsordningen

Den lagstiftning som föreslås i denna proposition bedöms uppfylla de krav som ställs i Europadomstolens avgörandepraxis och grundlagsutskottets tolkningspraxis vad gäller iakttagande av de grundläggande och mänskliga rättigheterna. Europadomstolens avgörandepraxis, som det hänvisats till ovan i detta avsnitt (Förhållande till grundlagen samt lagstiftningsordning), beskrivs närmare i avsnitt 2.4.

De lagförslag som ingår i propositionen kan enligt regeringens uppfattning behandlas i vanlig lagstiftningsordning frånsett de föreslagna befogenhetsbestämmelser som innebär ingrepp i hemligheten i fråga om förtroliga meddelanden, vilken tryggas i 10 § 2 mom. i grundlagen

Till dessa bestämmelser hör 6 § (teleavlyssning och inhämtande av information i stället för teleavlyssning), 7 § (teleövervakning), 11 § (teknisk avlyssning), 31 § (kopiering av försändelser) i det föreslagna 5 a kap. i polislagen och 7 § (underrättelseinhämtning som avser datatrafik) i den föreslagna lagen om civil underrättelseinhämtning avseende datatrafik.

Det är emellertid möjligt att anta dessa i vanlig lagstiftningsordning på grundval av den nya begränsningsgrund rörande den nationella säkerheten som enligt förslaget till ändring av grundlagen ska ingå i 10 § 4 mom.

De befogenheter som räknas upp ovan är kopplade till den föreslagna ändringen i grundlagen. Därför och även på grund av övriga konstitutionella aspekter som sammanhänger med propositionen, anser regeringen det ändamålsenligt att riksdagen begär utlåtande om propositionen av grundlagsutskottet.

Alla regeringspropositioner som har samband med underrättelseverksamhet är beroende av varandra, och de ska enligt regeringens uppfattning föras till grundlagsutskottet för att behandlas tillsammans.

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

Lagförslag

1.

Lag

om ändring av polislagen

I enlighet med riksdagens beslut

ändras i polislagen (872/2011) 1 kap. 1 § 1 mom., 5 kap. 5 § 1 mom., 7 § 1 och 3 mom., 8 § 1 mom., 10 § 1–4 mom. och 6 mom., 12 § 1 och 3 mom., 14 § 1 och 3 mom., 16 § 1 mom., 18 § 2 och 4 mom., 20 § 1, 2 och 4 mom., 22 § 1, 2 och 4 mom., 24 § 1 och 3 mom., 25 § 3 mom., 32 § 1 mom., 36 § 1 och 3 mom., 38 § 1 mom., 39 § 1 mom., 40 § 1 mom., 42 § 1 mom., 44 § 1 mom., 47 § 2 mom., 48 § 1 mom., 52 och 57 §, 58 § 1 mom., 61 § 2 mom. och den finska språkdräkten i 63 § 2 mom., den finska språkdräkten i 9 kap. 8 § och 9 § 2 mom. samt 9 kap. 10 § 2 mom.,

av dem 5 kap. 7 § 3 mom., 10 § 3 och 6 mom., 12 § 3 mom., 18 § 4 mom., 20 § 4 mom., 22 § 4 mom., 47 § 2 mom. och 58 § 1 mom. sådana de lyder i lag 1168/2013, och

fogas till lagen ett nytt 5 a kap. som följer:

1 kap.

Allmänna bestämmelser

1 §

Polisens uppgifter

Polisens uppgift är att trygga rätts- och samhällsordningen, skydda den nationella säkerheten, upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning. Polisen ska upprätthålla säkerheten i samarbete med andra myndigheter samt med sammanslutningar och invånarna och sköta det internationella samarbete som hör till dess uppgifter.

— —

5 kap.

Hemliga metoder för inhämtande av information

5 §

Teleavlyssning och dess förutsättningar

Med *teleavlyssning* avses att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett i 3 § 43 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) avsett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 8 §. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas göra sig skyldig till ett brott som avses i 2 mom.

— —

7 §

Beslut om teleavlyssning och motsvarande inhämtande av information

Beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning ska fattas av domstol på yrkande av en polisman som avses i 2 kap. 9 § 1 mom. 1 punkten i tvångsmedelslagen (*anhållningsberättigad polisman*) eller på yrkande av chefen eller en biträdande chef för skyddspolisen eller en avdelningschef, överinspektör eller inspektör vid skyddspolisen (*polisman som hör till befälet vid skyddspolisen*).

— —

I ett yrkande och i ett beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning ska följande nämnas:

1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden,

2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,

3) de fakta som misstanken mot personen och förutsättningarna för teleavlyssningen eller för inhämtandet av information i stället för teleavlyssning grundar sig på,

4) giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning eller inhämtande av information enligt 6 § 2 mom.,

5) den teleadress eller teleterminalutrustning som åtgärden riktas mot,

6) den i 1 mom. avsedda polisman som leder och övervakar utförandet av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning,

7) eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.

8 §

Teleövervakning och dess förutsättningar

Med *teleövervakning* avses att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät som avses i 5 § eller som har mottagits till en sådan adress eller utrustning samt att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att användningen av adressen eller utrustningen tillfälligt förhindras. Med *identifieringsuppgifter* avses sådana uppgifter om ett meddelande som kan förknippas med en i 3 § 7 punkten i lagen om tjänster inom elektronisk kommunikation avsedd användare eller med en i 30 punkten i den paragrafen avsedd abonnent och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.

— —

10 §

Beslut om teleövervakning

Beslut om teleövervakning enligt 8 § 2 och 5 mom. samt 9 § 1, 4 och 5 punkten och om teleövervakning i de fall som avses i 3 § ska fattas av domstol på yrkande av en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen.

Om ett ärende som gäller annan i 1 mom. avsedd teleövervakning än sådan som avses i 3 § inte tål uppskov, får en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen besluta om teleövervakning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

Chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning ska besluta om teleövervakning som avses i 8 § 4 mom. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen besluta om teleövervakningen till dess att chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning har avgjort ärendet om teleövervakning. Ärendet ska föras till nämnda polisman för avgörande så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

En anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen ska besluta om teleövervakning som avses i 8 § 3 mom. och 9 § 2 och 3 punkten.

— —

I ett yrkande och i ett beslut om teleövervakning ska följande nämnas:

1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden,

2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,

3) de fakta som misstanken mot personen och förutsättningarna för teleövervakning grundar sig på,

4) samtycke, om detta är ett villkor för teleövervakningen,

5) tillståndets giltighetstid med angivande av klockslag,

6) den teleadress eller teleterminalutrustning som åtgärden riktas mot,

7) den polisman som leder och övervakar utförandet av teleövervakningen och som avses i 7 § 1 mom.,

8) eventuella begränsningar och villkor för teleövervakningen.

12 §

Beslut om inhämtande av basstationsuppgifter

Beslut om inhämtande av basstationsuppgifter ska fattas av domstol på yrkande av en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen besluta om inhämtande av basstationsuppgifter till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

— —

I ett yrkande och i ett beslut om inhämtande av basstationsuppgifter ska följande nämnas:

1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden,

2) de fakta som ligger till grund för förutsättningarna för inhämtande av basstationsuppgifter,

3) den tidsperiod som tillståndet gäller,

4) vilken basstation tillståndet gäller,

5) den polisman som leder och övervakar inhämtandet av basstationsuppgifter och som avses i 7 § 1 mom.,

6) eventuella begränsningar och villkor för inhämtandet av basstationsuppgifter.

14 §

Beslut om systematisk observation

Beslut om systematisk observation ska fattas av en anhållningsberättigad polisman eller av en polisman som hör till befälet vid skyddspolisen.

— —

Beslut om systematisk observation ska fattas skriftligen. I beslutet ska följande nämnas:

1) det brott som ligger till grund för åtgärden samt brottstidpunkten,
2) den person som med fog kan antas begå det brott som avses i 1 punkten,
3) de fakta som misstanken mot personen och den systematiska observationen grundar sig på,
4) tillståndets giltighetstid,
5) den polisman som leder och övervakar genomförandet av den systematiska observationen och som avses i 7 § 1 mom.,
6) eventuella begränsningar och villkor för den systematiska observationen.

16 §

Beslut om förtäckt inhämtande av information

Beslut om förtäckt inhämtande av information ska fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning eller av en för uppdraget förordnad sådan anhållningsberättigad polisman eller polisman som hör till befälet vid skyddspolisen som särskilt utbildats för hemligt inhämtande av information.

— —

18 §

Beslut om teknisk avlyssning

— —

Beslut om teknisk avlyssning som avses i 17 § 5 mom. och om annan än i 1 mom. avsedd teknisk avlyssning ska fattas av en anhållningsberättigad polisman eller av en polisman som hör till befälet vid skyddspolisen.

— —

I ett yrkande och i ett beslut om teknisk avlyssning ska följande nämnas:
1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden,
2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,
3) de fakta som misstanken mot personen och förutsättningarna för den tekniska avlyssningen grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,
5) det utrymme eller den plats av annat slag som avlyssningen riktas mot,
6) den polisman som leder och övervakar genomförandet av den tekniska avlyssningen och som avses i 7 § 1 mom.,
7) eventuella begränsningar och villkor för den tekniska avlyssningen.

20 §

Beslut om optisk observation

Beslut om optisk observation ska fattas av domstol på yrkande av en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen, om observationen riktas mot ett sådant hemfridsskyddat utrymme eller en annan plats som avses i 24 kap. 11 § i strafflagen eller mot en person som berövats sin frihet på grund av brott.

Beslut om optisk observation som avses i 19 § 5 mom. och om annan än i 1 mom. avsedd optisk observation ska fattas av en anhållningsberättigad polisman eller av en polisman som hör till befälet vid skyddspolisen.

— —

I ett yrkande och i ett beslut om optisk observation ska följande nämnas:

1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden,
2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,
3) de fakta som misstanken mot personen och förutsättningarna för den optiska observationen grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,
5) det utrymme eller den plats av annat slag som observationen riktas mot,
6) den polisman som leder och övervakar genomförandet av den optiska observationen och som avses i 7 § 1 mom.,
7) eventuella begränsningar och villkor för den optiska observationen.

22 §

Beslut om teknisk spårning

Beslut om teknisk spårning av en person ska fattas av domstol på yrkande av en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen besluta om sådan spårning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

Beslut om teknisk spårning som avses i 21 § 4 mom. och om annan än i 1 mom. avsedd teknisk spårning ska fattas av en anhållningsberättigad polisman eller av en polisman som hör till befälet vid skyddspolisen.

— —

I ett yrkande och i ett beslut om teknisk spårning ska följande nämnas:
1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden,
2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,
3) de fakta som misstanken mot personen och förutsättningarna för den tekniska spårningen grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,
5) det föremål, det ämne eller den egendom som spårningen riktas mot,
6) den polisman som leder och övervakar genomförandet av den tekniska spårningen och som avses i 7 § 1 mom.,
7) eventuella begränsningar och villkor för den tekniska spårningen.

24 §

Beslut om teknisk observation av utrustning

Beslut om teknisk observation av utrustning ska fattas av domstol på yrkande av en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen besluta om teknisk observation av utrustning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

— —

I ett yrkande och i ett beslut om teknisk observation av utrustning ska följande nämnas:
1) det brott som ligger till grund för åtgärden samt brottstidpunkten,
2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,
3) de fakta som misstanken mot personen och förutsättningarna för den tekniska observationen av utrustning grundar sig på,

4) tillståndets giltighetstid med angivande av klockslag,
5) den tekniska anordning eller programvara som åtgärden riktas mot,
6) den polisman som leder och övervakar genomförandet av den tekniska observationen av utrustning och som avses i 7 § 1 mom.,
7) eventuella begränsningar och villkor för den tekniska observationen av utrustning.

25 §

Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning

— —

Beslut om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning ska fattas av en anhållningsberättigad polisman eller av en polisman som hör till befälet vid skyddspolisen.

32 §

Beslut om en täckoperation

Beslut om en täckoperation ska fattas av chefen för centralkriminalpolisen eller chefen för skyddspolisen. Beslut om en täckoperation som genomförs uteslutande i datanät får fattas också av chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning eller av en för uppdraget förordnad sådan anhållningsberättigad polisman eller polisman som hör till befälet vid skyddspolisen som särskilt utbildats för hemligt inhämtande av information.

— —

36 §

Beslut om bevisprovokation genom köp

Beslut om bevisprovokation genom köp ska fattas av chefen för centralkriminalpolisen eller chefen för skyddspolisen. Beslut om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten får fattas också av en för uppdraget förordnad sådan anhållningsberättigad polisman eller polisman som hör till befälet vid skyddspolisen som särskilt utbildats för hemligt inhämtande av information.

— —

Beslut om bevisprovokation genom köp ska fattas skriftligen. I beslutet ska följande nämnas:
1) det brott som ligger till grund för åtgärden,
2) den person som är föremål för bevisprovokationen,
3) de fakta som brottsmisstanken och förutsättningarna för bevisprovokationen grundar sig på,
4) de föremål, de ämnen, den egendom eller de tjänster som är föremål för bevisprovokationen,
5) syftet med bevisprovokationen,
6) beslutets giltighetstid,
7) den anhållningsberättigade polisman eller till befälet vid skyddspolisen hörande polisman som leder och övervakar genomförandet av bevisprovokationen,
8) eventuella begränsningar och villkor för bevisprovokationen.

38 §

Beslut om genomförande av bevisprovokation genom köp

Beslut om genomförande av bevisprovokation genom köp ska fattas skriftligen. Beslutet ska fattas av en sådan anhållningsberättigad polisman eller polisman som hör till befälet vid skyddspolisen som särskilt utbildats för hemligt inhämtande av information och som ansvarar för genomförandet av bevisprovokationen.

— —

39 §

Säkerheten för en polisman vid förtäckt inhämtande av information, en täckoperation och vid bevisprovokation genom köp

En anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen får besluta att en polisman som ska genomföra förtäckt inhämtande av information, en täckoperation eller bevisprovokation genom köp ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att polismannens säkerhet ska kunna tryggas.

— —

40 §

Användning av informationskällor och förutsättningar för styrd användning av informationskällor

Med *användning av informationskällor* avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av i 1 kap. 1 § avsedda uppgifter av personer som inte hör till polisen eller till någon annan myndighet (*informationskälla*).

— —

42 §

Beslut om styrd användning av informationskällor

Beslut om styrd användning av informationskällor ska fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning eller av en för uppdraget förordnad sådan anhållningsberättigad polisman eller polisman som hör till befälet vid skyddspolisen som särskilt utbildats för hemligt inhämtande av information.

— —

44 §

Beslut om kontrollerade leveranser

Beslut om kontrollerade leveranser som utförs av polisen ska fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning eller av en för uppdraget förordnad sådan anhållningsberättigad polisman eller polisman som hör till befälet vid skyddspolisen som särskilt utbildats för hemligt inhämtande av information. Det föreskrivs särskilt om andra myndigheters beslutsfattande om kontrollerade leveranser.

— —

47 §

Beslut om skyddande

— —

En sådan anhållningsberättigad polisman eller polisman som hör till befälet vid skyddspolisen som särskilt utbildats för hemligt inhämtande av information beslutar om annat än i 1 mom. avsett skyddande av inhämtande av information.

— —

48 §

Yppandeförbud som gäller hemligt inhämtande av information

En anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen får av viktiga skäl som hänför sig till förhindrande eller avslöjande av brott förbjuda en utomstående att röja sådana omständigheter om användningen av hemligt inhämtande av information som denne fått kännedom om. Det förutsätts dessutom att den utomstående med anledning av sitt uppdrag eller sin ställning har bistått eller blivit ombedd att bistå vid hemligt inhämtande av information.

— —

52 §

Undersökning av upptagningar

Upptagningar som uppkommit vid hemligt inhämtande av information får undersökas endast av domstol och en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen. Enligt förordnande av den anhållningsberättigade polismannen eller den polisman som hör till befälet vid skyddspolisen eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en expert eller av någon annan som anlitas för inhämtande av information.

57 §

Utplåning av information som erhållits i en brådskande situation

Om en anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen i en brådskande situation enligt 10 § 2 mom., 12 § 1 mom., 22 § 1 mom. eller 24 § 1 mom. har beslutat att teleövervakning, inhämtande av basstationsuppgifter, teknisk spårning av en person eller teknisk observation av utrustning ska inledas men domstolen anser att det inte har funnits förutsättningar för åtgärden, ska inhämtandet av information avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Information som fåtts på detta sätt får dock användas på samma villkor som överskottsinformation får användas enligt 54 §.

58 §

Underrättelse om hemligt inhämtande av information

Den som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk observation och kontrollerade leveranser ska utan dröjsmål un-

derrättas om detta skriftligen efter det att syftet med inhämtandet av information har nåtts. Personen i fråga ska dock underrättas om det hemliga inhämtandet av information senast ett år efter att det har upphört.

— —

61 §

Teleföretags skyldighet att biträda samt tillträde till vissa utrymmen

— —

Polisen, den som utför åtgärden och den biträdande personalen har rätt att för att göra de kopplingar som behövs för teleavlyssning få tillträde också till andra utrymmen än de som är i teleföretagets besittning, dock inte till utrymmen som används för stadigvarande boende. En anhållningsberättigad polisman eller en polisman som hör till befälet vid skyddspolisen beslutar om åtgärden. Det föreskrivs särskilt om husrannsakan.

5 a kap.

Civil underrättelseinhämtning

1 §

Tillämpningsområde

Detta kapitel innehåller bestämmelser om skyddspolisens inhämtande och nyttjande av information för att den nationella säkerheten ska kunna skyddas och den högsta statsledningens beslutsfattande stödjas samt för att andra myndigheter ska kunna utföra de lagstadgade uppgifter som hänför sig till den nationella säkerheten (*civil underrättelseinhämtning*).

2 §

Metoder för civil underrättelseinhämtning

Metoder för civil underrättelseinhämtning är teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, teknisk spårning, teknisk observation av utrustning, inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp och styrd användning av informationskällor.

Metoder för civil underrättelseinhämtning är även i detta kapitel avsedd platsspecifik underrättelseinhämtning och kopiering samt i detta kapitel avsett kvarhållande av en försändelse för kopiering och inhämtande av information från privata sammanslutningar.

I detta kapitel föreskrivs om förutsättningarna för användning av de i 1 mom. avsedda metoderna för underrättelseinhämtning och av platsspecifik underrättelseinhämtning, kopiering, kvarhållande av en försändelse för kopiering och rätt att få information av privata sammanslutningar vid civil underrättelseinhämtning.

Bestämmelser om underrättelseinhämtning som avser datatrafik som en metod för civil underrättelseinhämtning finns i lagen om civil underrättelseinhämtning avseende datatrafik (/).

3 §

Föremål för civil underrättelseinhämtning

Genom civil underrättelseinhämtning får information inhämtas om
1) terrorism,
2) utländsk underrättelseverksamhet,
3) planering, tillverkning, spridning och användning av massförstörelsevapen,
4) planering, tillverkning, spridning och användning av sådana produkter med dubbel användning som avses i 2 § i lagen om kontroll av export av produkter med dubbel användning (562/1996),
5) verksamhet som hotar den demokratiska samhällsordningen,
6) verksamhet som hotar ett stort antal människors liv eller hälsa eller samhällets vitala funktioner,
7) en främmande stats verksamhet som kan orsaka skada för Finlands internationella relationer, ekonomiska intressen eller andra viktiga intressen,
8) en kris som hotar internationell fred och säkerhet,
9) verksamhet som hotar säkerheten vid internationella krishanteringsinsatser,
10) verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och deltar i annan internationell verksamhet,
11) internationell organiserad brottslighet som hotar samhällsordningen.

4 §

Förutsättningar för användning av metoderna för underrättelseinhämtning

En allmän förutsättning för användning av en metod för civil underrättelseinhämtning är att det med fog kan antas att man genom metoden kan få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten.

Utöver vad som nedan föreskrivs om särskilda förutsättningar för användning av metoder för underrättelseinhämtning får teleavlyssning, inhämtande av information i stället för teleavlyssning, systematisk observation, teknisk avlyssning, optisk observation, teknisk spårning av personer, teknisk observation av utrustning, täckoperationer, bevisprovokation genom köp, styrd användning av informationskällor och platsspecifik underrättelseinhämtning användas inom civil underrättelseinhämtning endast om dessa metoder med fog kan antas vara av synnerlig vikt för att få information om sådan verksamhet som avses i 1 mom. För täckoperationer och bevisprovokation genom köp förutsätts dessutom att användningen av metoden är nödvändig. En förutsättning för täckoperationer är dessutom att inhämtandet av information måste anses vara behövligt på grund av att verksamheten är planmässig, organiserad eller yrkesmässig eller på grund av att det kan antas att den fortsätter eller upprepas.

Om en metod för underrättelseinhämtning riktas mot en statlig aktör eller en aktör som är jämställbar med en sådan, ska på förutsättningarna för användningen av metoderna för underrättelseinhämtning tillämpas bara det som föreskrivs i 1 mom.

Metoder för underrättelseinhämtning får inte riktas mot ett utrymme som används för stadigvarande boende. Täckoperationer och bevisprovokation genom köp får dock företas i en bostad om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden.

Användningen av en metod för underrättelseinhämtning ska avslutas före utgången av den tid som anges i beslutet, om syftet med användningen har nåtts eller om det inte längre finns förutsättningar för att använda metoden.

5 §

Fortsatt inhämtande av information för förhindrande och avslöjande av vissa brott

Om det vid civil underrättelseinhämtning, medan en metod för underrättelseinhämtning används, framkommer att en person med fog kan antas göra sig skyldig till ett brott som nämns i 5 kap. 3 § eller till högförräderi, grovt högförräderi eller olaglig militär verksamhet eller det kan antas att ett sådant brott har begåtts och det genom användning av metoden för underrättelseinhämtning inte längre kan antas att man får information om den verksamhet som allvarligt hotar den nationella säkerheten och som låg till grund för tillståndet eller beslutet, får skyddspolisen fortsätta att använda metoden som en hemlig metod för inhämtande av information i avsikt att förhindra och avslöja brott under giltighetstiden för det tillstånd som fattats med stöd av detta kapitel, dock högst i en månads tid. Då ska ärendet inom den nämnda tiden föras för avgörande till den myndighet som är behörig att fatta beslut om användning av den aktuella metoden för inhämtande av information.

6 §

Beslut om teleavlyssning och motsvarande inhämtande av information vid civil underrättelseinhämtning

Beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen.

Tillstånd till teleavlyssning och till inhämtande av information i stället för teleavlyssning får ges för högst sex månader åt gången. När åtgärden gäller en person får tillstånd ges för högst tre månader åt gången.

I ett yrkande och i ett beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning ska följande nämnas:

1) den verksamhet som avses i 3 §,

2) den person, teleadress eller teleterminalutrustning som åtgärden riktas mot,

3) de fakta som förutsättningarna för och inriktningen av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning grundar sig på,

4) giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning och till inhämtande av information i stället för teleavlyssning,

5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar teleavlyssningen eller inhämtandet av information i stället för teleavlyssning,

6) eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.

7 §

Beslut om teleövervakning vid civil underrättelseinhämtning

Beslut om teleövervakning vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ett ärende som gäller teleövervakning inte tål uppskov, får chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om teleövervakning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

För inhämtande av uppgifter om verksamhet som är föremål för civil underrättelseinhämtning får skyddspolisen med samtycke av den som innehar en teleadress eller teleterminalutrustning rikta teleövervakning mot teleadressen eller teleterminalutrustningen.

Chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om sådan teleövervakning som avses i 2 mom.

Tillstånd får beviljas och beslut fattas för högst sex månader åt gången, och tillståndet eller beslutet får gälla även en viss tid före tillståndet beviljades eller beslutet fattades, vilken kan vara längre än sex månader.

I ett yrkande och i ett beslut om teleövervakning ska följande nämnas:

1) åtgärden, dess syfte samt den verksamhet som avses i 3 §,
2) den person, teleadress eller teleterminalutrustning som åtgärden riktas mot,
3) de fakta som förutsättningarna för och inriktningen av teleövervakningen grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,
5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar teleövervakningen,
6) eventuella begränsningar och villkor för teleövervakningen.

8 §

Beslut om inhämtande av basstationsuppgifter vid civil underrättelseinhämtning

Beslut om inhämtande av basstationsuppgifter vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en polisman som hör till befälet vid skyddspolisen besluta om inhämtande av basstationsuppgifter till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

Tillstånd beviljas för en viss tidsperiod.

I ett yrkande och i ett beslut om inhämtande av basstationsuppgifter ska följande nämnas:

1) den verksamhet som avses i 3 §,
2) vilken basstation tillståndet gäller,
3) de fakta som förutsättningarna för och inriktningen av inhämtandet av basstationsuppgifter grundar sig på,
4) den tidsperiod som tillståndet gäller,
5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar inhämtandet av basstationsuppgifter,
6) eventuella begränsningar och villkor för inhämtandet av basstationsuppgifter.

9 §

Beslut om systematisk observation vid civil underrättelseinhämtning

Beslut om systematisk observation vid civil underrättelseinhämtning ska fattas av en polisman som hör till befälet vid skyddspolisen.

Beslut om systematisk observation får fattas för högst sex månader åt gången.

Beslut om systematisk observation ska fattas skriftligen. I beslutet ska följande nämnas:

1) den verksamhet som avses i 3 §,
2) den person eller grupp av personer som åtgärden riktas mot,
3) de fakta som förutsättningarna för och inriktningen av den systematiska observationen grundar sig på,
4) tillståndets giltighetstid,

5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar utförandet av den systematiska observationen,
6) eventuella begränsningar och villkor för den systematiska observationen.

10 §

Beslut om förtäckt inhämtande av information vid civil underrättelseinhämtning

Beslut om förtäckt inhämtande av information vid civil underrättelseinhämtning ska fattas av chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning.
Beslutet om förtäckt inhämtande av information ska fattas skriftligen. I beslutet ska följande nämnas:
1) åtgärden och dess syfte tillräckligt specificerat,
2) den verksamhet som avses i 3 §,
3) den person eller grupp av personer som åtgärden riktas mot,
4) de fakta som förutsättningarna för och inriktningen av det förtäckta inhämtandet av information grundar sig på,
5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar det förtäckta inhämtandet av information,
6) den planerade tidpunkten för genomförandet av åtgärden,
7) eventuella begränsningar och villkor för det förtäckta inhämtandet av information.
Vid förändrade omständigheter ska beslutet vid behov ses över.
Om åtgärden inte tål uppskov, behöver ett beslut som avses i 1 mom. inte upprättas i skriftlig form före det förtäckta inhämtandet av information. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter det att åtgärden har vidtagits.

11 §

Beslut om teknisk avlyssning vid civil underrättelseinhämtning

Beslut om teknisk avlyssning som riktas mot en frihetsberövad person vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om teknisk avlyssning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.
En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om annan teknisk avlyssning än sådan som avses i 1 mom.
Tillstånd får ges och beslut fattas för högst sex månader åt gången.
I ett yrkande och i ett beslut om teknisk avlyssning ska följande nämnas:
1) den verksamhet som avses i 3 §,
2) den person eller grupp av personer eller det utrymme eller den plats av annat slag som åtgärden riktas mot,
3) de fakta som förutsättningarna för och inriktningen av den tekniska avlyssningen grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,
5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar den tekniska avlyssningen,
6) eventuella begränsningar och villkor för den tekniska avlyssningen.

12 §

Beslut om optisk observation vid civil underrättelseinhämtning

Beslut om optisk observation som riktas mot en frihetsberövad person vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om optisk observation till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om annan optisk observation än sådan som avses i 1 mom.

Tillstånd får ges och beslut fattas för högst sex månader åt gången.

I ett yrkande och i ett beslut om optisk observation ska följande nämnas:

1) den verksamhet som avses i 3 §,

2) den person eller grupp av personer eller det utrymme eller den plats av annat slag som åtgärden riktas mot,

3) de fakta som förutsättningarna för och inriktningen av den optiska observationen grundar sig på,

4) tillståndets giltighetstid med angivande av klockslag,

5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar den optiska observationen,

6) eventuella begränsningar och villkor för den optiska observationen.

13 §

Beslut om teknisk spårning vid civil underrättelseinhämtning

Beslut om teknisk spårning av en person vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om teknisk spårning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

En polisman som hör till befälet vid skyddspolisen beslutar om annan teknisk spårning än sådan som avses i 1 mom.

Tillstånd får ges och beslut fattas för högst sex månader åt gången.

I ett yrkande och i ett beslut om teknisk spårning ska följande nämnas:

1) den verksamhet som avses i 3 §,

2) den person, det föremål, det ämne eller den egendom som åtgärden riktas mot,

3) de fakta som förutsättningarna för och inriktningen av den tekniska spårningen grundar sig på,

4) tillståndets giltighetstid med angivande av klockslag,

5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar den tekniska spårningen,

6) eventuella begränsningar och villkor för den tekniska spårningen.

14 §

Beslut om teknisk observation av utrustning vid civil underrättelseinhämtning

Beslut om teknisk observation av utrustning vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en polisman som hör till befälet vid skyddspolisen besluta om teknisk observation av utrustning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

Tillstånd får beviljas för högst sex månader åt gången.

I ett yrkande och i ett beslut om teknisk observation av utrustning ska följande nämnas:

1) den verksamhet som avses i 3 §,

2) den tekniska anordning eller programvara som åtgärden riktas mot,

3) de fakta som förutsättningarna för och inriktningen av den tekniska observationen av utrustning grundar sig på,

4) tillståndets giltighetstid med angivande av klockslag,

5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar den tekniska observationen av utrustning,

6) eventuella begränsningar och villkor för den tekniska observationen av utrustning.

15 §

Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning vid civil underrättelseinhämtning

Skyddspolisen får vid civil underrättelseinhämtning inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning med en teknisk anordning.

Kommunikationsverket ska kontrollera att den tekniska anordningen inte på grund av sina egenskaper orsakar skadliga störningar i anordningar eller tjänster i allmänna kommunikationsnät.

Beslut om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning fattas av en polisman som hör till befälet vid skyddspolisen.

16 §

Installation och avinstallation av anordningar, metoder eller programvara vid civil underrättelseinhämtning

En tjänsteman som är anställd vid skyddspolisen har vid civil underrättelseinhämtning rätt att placera en anordning, metod eller programvara som används för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, optisk observation, teknisk spårning eller teknisk observation av utrustning på eller i föremål, ämnen, egendom, utrymmen, platser eller informationssystem som åtgärden riktas mot, om det behövs för användningen av metoden för underrättelseinhämtning. För att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran har en tjänsteman som är anställd vid skyddspolisen då rätt att i hemlighet ta sig in i ett ovan nämnt utrymme eller på en ovan nämnd plats eller i ett ovan nämnt informationssystem och att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemens säkerhetssystem.

Anordningar, metoder och programvara som används för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, optisk observation, teknisk spårning eller teknisk observation av utrustning får installeras i utrymmen som an-

vänds för stadigvarande boende endast om domstolen har gett tillstånd till det på yrkande av en polisman som hör till befälet vid skyddspolisen.

17 §

Framställning om och plan för en täckoperation vid civil underrättelseinhämtning

I en framställning om en täckoperation vid civil underrättelseinhämtning ska följande nämnas:
1) den som föreslagit åtgärden,
2) den person eller grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information,
3) den verksamhet som avses i 3 §,
4) de fakta som förutsättningarna för och inriktningen av täckoperationen grundar sig på,
5) syftet med täckoperationen,
6) behovet av täckoperationen,
7) övriga uppgifter som behövs för att bedöma förutsättningarna för täckoperationen.

Över en täckoperation ska en sådan skriftlig plan göras upp som innehåller väsentlig och tillräckligt detaljerad information för beslutsfattandet om och genomförandet av täckoperationen. Vid förändrade omständigheter ska planen vid behov ses över.

18 §

Beslut om en täckoperation vid civil underrättelseinhämtning

Beslut om en sådan täckoperation som avses i 17 § ska fattas av chefen för skyddspolisen. Beslut om täckoperationer som genomförs uteslutande i datanät får fattas också av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning.

Ett beslut om en täckoperation får vara i kraft högst sex månader åt gången.

Beslut om en täckoperation ska fattas skriftligen. I beslutet ska följande nämnas:
1) den som föreslagit åtgärden,
2) den polisman som ansvarar för genomförandet av täckoperationen,
3) identifikationsuppgifterna för de polismän som genomför täckoperationen,
4) den verksamhet som avses i 3 §,
5) den person eller grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information,
6) de fakta som förutsättningarna för och inriktningen av täckoperationen grundar sig på,
7) täckoperationens syfte och genomförandeplan,
8) tillståndets giltighetstid,
9) eventuella begränsningar och villkor för täckoperationen.

Vid förändrade omständigheter ska beslutet vid behov ses över. Beslut om avslutande av en täckoperation ska fattas skriftligen.

19 §

Brottsförbud vid civil underrättelseinhämtning

En polisman vid skyddspolisen som företar en täckoperation vid civil underrättelseinhämtning får inte begå brott eller ta initiativ till ett brott.

Om en polisman vid skyddspolisen som företar en täckoperation begår en trafikförseelse, en ordningsförseelse eller något annat jämförbart brott för vilket det föreskrivna straffet är ord-

ningsbot, går polismannen fri från straffansvar, om gärningen har varit nödvändig för att syftet med täckoperationen ska nås eller för att inhämtandet av information inte ska avslöjas.

20 §

Beslut om bevisprovokation genom köp vid civil underrättelseinhämtning

Beslut om bevisprovokation genom köp vid civil underrättelseinhämtning ska fattas av chefen för skyddspolisen. Beslut om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten får fattas också av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning.

Beslut om bevisprovokation genom köp får meddelas för högst sex månader åt gången.

Beslut om bevisprovokation genom köp ska fattas skriftligen. I beslutet ska följande nämnas:

1) den verksamhet som avses i 3 §,
2) den person som är föremål för bevisprovokation,
3) de fakta som förutsättningarna för och inriktningen av bevisprovokationen grundar sig på,
4) de föremål, de ämnen, den egendom eller de tjänster som är föremål för bevisprovokationen,
5) syftet med bevisprovokationen,
6) tillståndets giltighetstid,
7) den till befälet vid skyddspolisen hörande polisman som leder och övervakar bevisprovokationen,
8) eventuella begränsningar och villkor för bevisprovokationen.

21 §

Plan för genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning

Över genomförandet av bevisprovokation genom köp vid civil underrättelseinhämtning ska det upprättas en skriftlig plan, om detta behövs med hänsyn till operationens omfattning eller andra motsvarande skäl.

Vid förändrade omständigheter ska planen för genomförande av bevisprovokationen vid behov ses över.

22 §

Beslut om genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning

Beslut om genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning ska fattas skriftligen. Beslutet ska fattas av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och är förtrogen med användningen av metoder för underrättelseinhämtning och som ansvarar för genomförandet av bevisprovokationen.

I beslutet ska följande nämnas:

1) den polisman som beslutat om bevisprovokationen genom köp samt beslutets datum och innehåll,
2) identifikationsuppgifterna för de polismän som genomför bevisprovokationen,
3) hur det har säkerställts att bevisprovokationen inte får den som är föremål för åtgärden eller någon annan att begå ett brott som denne annars inte skulle begå,
4) eventuella begränsningar och villkor för bevisprovokationen.

Om åtgärden inte tål uppskov, behöver ett beslut som avses i 2 mom. inte upprättas i skriftlig form före bevisprovokationen. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter bevisprovokationen.

Vid förändrade omständigheter ska beslutet om genomförande av bevisprovokationen vid behov ses över.

23 §

Säkerheten för polismän vid förtäckt inhämtande av information, täckoperationer, bevisprovokation genom köp och användning av informationskällor vid civil underrättelseinhämtning

En polisman som hör till befälet vid skyddspolisen får besluta att en polisman som ska genomföra sådant förtäckt inhämtande av information, en sådan täckoperation eller sådan bevisprovokation genom köp eller förbereda eller genomföra sådan användning av informationskällor som avses i detta kapitel ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att polismannens säkerhet ska kunna tryggas.

Avlyssningen och observationen får upptas. Upptagningarna ska utplånas så snart de inte behövs för att trygga polismannens säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har samband med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller avskrivits.

24 §

Beslut om styrd användning av informationskällor vid civil underrättelseinhämtning

Beslut om styrd användning av informationskällor vid civil underrättelseinhämtning fattas av chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning.

Ett beslut om styrd användning av informationskällor får vara i kraft högst sex månader åt gången.

Beslut om styrd användning av informationskällor ska fattas skriftligen. I beslutet ska följande nämnas:

1) den som föreslagit åtgärden,
2) den polisman som ansvarar för genomförandet av inhämtandet av information,
3) identifikationsuppgifterna för informationskällan,
4) den verksamhet som avses i 3 §,
5) de fakta som förutsättningarna för och inriktningen av den styrda användningen av informationskällor grundar sig på,
6) syftet med inhämtandet av information och planen för genomförandet av detta,
7) tillståndets giltighetstid,
8) eventuella begränsningar och villkor för den styrda användningen av informationskällor.

Vid förändrade omständigheter ska beslutet vid behov ses över. Beslut om avslutande av styrd användning av en informationskälla ska fattas skriftligen.

I fråga om registrering av uppgifter om informationskällor i ett personregister och betalning av arvode tillämpas vad som föreskrivs i 5 kap. 41 §.

25 §

Tryggande av informationskällor vid civil underrättelseinhämtning

Vid civil underrättelseinhämtning kan skyddspolisen med en informationskällas samtycke övervaka informationskällans bostad, eller något annat utrymme som informationskällan använder för boende, och dess omedelbara närmiljö med kamera eller någon annan teknisk anordning, metod eller programvara som placerats på platsen, om det behövs för att avvärja en

fara som hotar informationskällans liv eller hälsa. Utomstående behöver inte upplysas om att informationskällan tryggas.

Övervakningen ska avslutas utan dröjsmål, om den inte längre behövs för att avvärja en fara som hotar informationskällans liv eller hälsa.

Upptagningar som uppkommit vid övervakning enligt 1 mom. ska utplånas så snart de inte behövs för att trygga informationskällans säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har samband med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller avskrivits.

En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning får besluta att en informationskälla, med informationskällans samtycke, ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen i ett enskilt fall är nödvändig för att informationskällans säkerhet ska kunna tryggas. Avlyssningen och observationen får upptas. Upptagningarna ska utplånas så snart de inte behövs för att trygga informationskällans säkerhet.

Chefen för skyddspolisen får besluta att en informationskälla ges falska, vilseledande eller förtäckta uppgifter eller registeranteckningar, som får användas i ett enskilt fall, eller att falska handlingar får upprättas för att användas av informationskällan, om det är nödvändigt för att för att skydda informationskällans liv och hälsa. En registeranteckning ska rättas när förutsättningarna enligt detta moment inte längre finns.

26 §

Platsspecifik underrättelseinhämtning

Med *platsspecifik underrättelseinhämtning* avses underrättelseinhämtning för att hitta föremål, egendom, handlingar eller information eller utröna omständigheter på någon annan plats än en plats som används för stadigvarande boende eller en plats beträffande vilken det finns anledning att anta att underrättelseinhämtningen kommer att omfatta information som någon enligt 17 kap. 11, 13, 14, 16, 20 eller 21 § eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om.

27 §

Beslut om platsspecifik underrättelseinhämtning vid civil underrättelseinhämtning

Beslut om platsspecifik underrättelseinhämtning vid civil underrättelseinhämtning ska fattas av domstol, om den riktas mot någon annan hemfridsskyddad plats än ett utrymme som används för stadigvarande boende eller mot en plats som allmänheten inte har tillträde till eller dit tillträdet för allmänheten har begränsats eller förhindrats under den tid den platsspecifika underrättelseinhämtningen genomförs, på yrkande av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning.

Om det ärende som avses i 1 mom. inte tål uppskov, får chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om platsspecifik underrättelseinhämtning till dess att domstolen har avgjort yrkandet. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

Chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om annan platsspecifik underrättelseinhämtning än sådan som avses i 1 mom.

Ett beslut om platsspecifik underrättelseinhämtning får vara i kraft högst en månad åt gången.

I ett yrkande och i ett beslut om platsspecifik underrättelseinhämtning ska tillräckligt noggrant specificeras

1) den verksamhet som avses i 3 §,

2) den plats som är föremål för den platsspecifika underrättelseinhämtningen,

3) de fakta utifrån vilka det anses finnas förutsättningar för platsspecifik underrättelseinhämtning,

4) vad som söks, i den utsträckning det är möjligt att ange, genom den platsspecifika underrättelseinhämtningen,

5) eventuella begränsningar i den platsspecifika underrättelseinhämtningen.

När sakens brådskande natur kräver det får ett beslut om platsspecifik underrättelseinhämtning dokumenteras efter det att den platsspecifika underrättelseinhämtningen har genomförts.

Om det medan en platsspecifik underrättelseinhämtning pågår framkommer att underrättelseinhämtningen har omfattat sådan information som någon enligt 17 kap. 11, 13, 14, 16, 20 eller 21 § eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om, ska underrättelseinhämtningen till denna del genast avslutas och de anteckningar och kopior som gäller informationen genast utplånas eller förstöras.

28 §

Kopiering vid civil underrättelseinhämtning

Skyddspolisen har vid civil underrättelseinhämtning rätt att kopiera handlingar och föremål.

29 §

Kopieringsförbud vid civil underrättelseinhämtning

En handling eller något annat objekt som avses i 26 § får inte kopieras vid civil underrättelseinhämtning, om objektet innehåller sådant som någon med stöd av 17 kap. 11, 13, 14, 16, 20 eller 21 § i rättegångsbalken har skyldighet eller rätt att vägra vittna om.

Om tystnadsplikten eller tystnadsrätten grundar sig på 17 kap. 11 § 2 eller 3 mom. i rättegångsbalken eller 13, 14, 16 eller 20 § i det kapitlet, är en förutsättning för förbudet utöver det som föreskrivs i 1 mom. dessutom att objektet innehas av en person som avses i bestämmelsen i fråga eller av någon som står i ett sådant förhållande till honom eller henne som avses i 17 kap. 22 § 2 mom. i rättegångsbalken, eller av den till vars förmån tystnadsplikten eller tystnadsrätten har föreskrivits.

Kopieringsförbud gäller dock inte, om

1) den i 17 kap. 11 § 2 eller 3 mom., 13 § 1 eller 3 mom., 14 § 1 mom. eller 16 § 1 mom. i rättegångsbalken avsedda person till vars förmån tystnadsplikten har föreskrivits samtycker till kopiering,

2) en i 17 kap. 20 § 1 mom. i rättegångsbalken avsedd person samtycker till kopiering.

30 §

Kopieringsförbud som gäller teleavlyssning, teleövervakning och basstationsuppgifter

Handlingar och data som innehas av ett i 3 § 27 punkten i lagen om tjänster inom elektronisk kommunikation avsett teleföretag (*teleföretag*) eller en i 36 punkten i den paragrafen avsedd sammanslutningsabonnent och som innehåller uppgifter om meddelanden som avses i 5 kap. 5 § 1 mom. i denna lag eller innehåller identifieringsuppgifter som avses i 5 kap. 8 § 1 mom. eller basstationsuppgifter som avses i 5 kap. 11 § 1 mom. får inte kopieras.

31 §

Kopiering av försändelser vid civil underrättelseinhämtning

Skyddspolisen har vid civil underrättelseinhämtning rätt att kopiera ett brev eller en annan försändelse innan den anländer till mottagaren.

32 §

Kvarhållande av försändelser för kopiering

Om det finns skäl att anta att ett brev eller någon annan försändelse som får kopieras vid civil underrättelseinhämtning kommer att anlända till eller redan finns vid ett verksamhetsställe för post, en järnvägsstation eller en del av en sådan eller ett verksamhetsställe som innehas av den som yrkesmässigt transporterar försändelser i samband med trafik eller annars, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning förordna att försändelsen ska hållas kvar på verksamhetsstället i fråga tills kopiering hinner utföras.

Det förordnande som avses i 1 mom. får meddelas för högst en månad räknat från det att chefen för verksamhetsstället har fått kännedom om förordnandet. Försändelsen får inte utan tillåtelse av den tjänsteman som avses i 1 mom. överlämnas till någon annan än tjänstemannen eller till den som han eller hon har utsett.

Chefen för verksamhetsstället ska genast underrätta den som meddelat föreläggandet om när försändelsen har anlänt. Denne ska utan ogrundat dröjsmål besluta om kopiering.

33 §

Beslut om kopiering

Beslut om kopiering vid civil underrättelseinhämtning ska fattas av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning.

Om ett ärende inte tål uppskov, får också någon annan polisman vid skyddspolisen än en sådan som avses i 1 mom. i ett enskilt fall besluta om kopiering, till dess att en tjänsteman som avses i 1 mom. har avgjort ärendet. Ärendet ska lämnas över till en polisman som avses i 1 mom. för avgörande så snart det är möjligt, dock senast 24 timmar efter det att metoden för inhämtande av information började användas.

34 §

Förstöring av kopior

En kopia ska förstöras utan dröjsmål, om det framgår att sådant material har kopierats som det är förbjudet att kopiera eller att informationen inte behövs för att skydda den nationella säkerheten.

35 §

Förfarandet i domstol i ärenden som gäller civil underrättelseinhämtning

Ett tillståndsärende som gäller en metod för civil underrättelseinhämtning ska handläggas av Helsingfors tingsrätt. Tingsrätten är domför med ordföranden ensam. Sammanträdet kan hållas

även vid en annan tidpunkt och på en annan plats än vad som förskrivs om en allmän underrätts sammanträde.

Ett yrkande om användning av en metod för underrättelseinhämtning ska göras skriftligen. Ett yrkande som gäller användning av en metod för underrättelseinhämtning ska utan dröjsmål tas upp till behandling i domstol i närvaro av den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman som är insatt i ärendet.

Ärendet ska avgöras skyndsamt. Behandlingen kan också ske med anlitande av videokonferens eller någon annan lämplig teknisk dataöverföring där de som deltar i behandlingen har sådan kontakt att de kan tala med och se varandra.

I fråga om varje metod för underrättelseinhämtning finns det särskilda bestämmelser om innehållet i beslutet. Beslutet ska meddelas omedelbart eller senast när behandlingen av de ärenden om metoder för underrättelseinhämtning som anknyter till samma underrättelsehelhet har avslutats.

Om domstolen har beviljat tillstånd till teleavlyssning eller teleövervakning, får den pröva och avgöra ett ärende som gäller beviljande av tillstånd i fråga om en ny person, teleadress eller teleterminalutrustning utan att den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman är närvarande, om det har förflutit mindre än sex månader från den muntliga förhandlingen av det tidigare tillståndsärendet. Ärendet kan behandlas utan att tjänstemannen är närvarande också om användningen av metoden för underrättelseinhämtning redan har avslutats.

Ett beslut i ett tillståndsärende får inte överklagas genom besvär. Klagan mot beslutet får anföras utan tidsbegränsning hos Helsingfors hovrätt. Klagan ska behandlas skyndsamt.

Vid handläggningen av ett ärende som gäller en metod för underrättelseinhämtning ska det fästas särskild vikt vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.

36 §

Skyddande av civil underrättelseinhämtning

Skyddspolisen får använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt upprätta och använda falska handlingar, om det är nödvändigt för att skydda den civila underrättelseinhämtningen.

En registeranteckning som avses i 1 mom. ska rättas när förutsättningarna enligt det momentet inte längre finns.

37 §

Beslut om skyddande

Beslut om registeranteckningar och upprättande av handlingar enligt 36 § 1 mom. ska fattas av chefen för skyddspolisen.

En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om annat än i 1 mom. avsett skyddande.

Den myndighet som har fattat beslut om registeranteckningar och upprättande av handlingar ska föra en förteckning över anteckningarna och handlingarna, övervaka användningen av dem samt se till att anteckningarna rättas.

38 §

Yppandeförbud vid civil underrättelseinhämtning

En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för civil underrättelseinhämtning får förbjuda en utomstående att röja sådana omständigheter om användningen av en metod för civil underrättelseinhämtning som denne fått kännedom om, om det är motiverat för att skydda metoden för underrättelseinhämtning. Det förutsätts dessutom att den utomstående med anledning av sitt uppdrag eller sin ställning har bistått eller blivit ombedd att bistå vid användningen av en metod för underrättelseinhämtning.

Ett yppandeförbud meddelas för högst ett år åt gången. Förbudet ska ges i skriftlig form och bevisligen delges den som förbudet gäller. I förbudet ska det specificeras de omständigheter som förbudet omfattar, nämnas förbudets giltighetstid och anges hotet om straff för överträdelse av förbudet.

Ett beslut om yppandeförbud får inte överklagas genom besvär. Den som har fått ett förbud får dock utan tidsbegränsning anföra klagan hos Helsingfors hovrätt. Klagan ska behandlas skyndsamt.

Till straff för överträdelse av yppandeförbudet döms enligt 38 kap. 1 eller 2 § i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans i lag.

Den som har fått ett yppandeförbud får trots 4 mom. meddela underrättelseombudsmannen om yppandeförbudet.

39 §

Beslut om användning av metoder för underrättelseinhämtning i vissa fall

Beslut om civil underrättelseinhämtning och användning av metoder för underrättelseinhämtning som sker utanför Finland ska fattas av chefen för skyddspolisen.

I fråga om innehållet i framställningar, planer, yrkanden och beslut som gäller användningen av metoder för underrättelseinhämtning tillämpas vad som i detta kapitel föreskrivs om framställningar, planer, yrkanden och beslut.

Bestämmelserna i 4 § 4 mom., 41, 44, 46 och 47 § i detta kapitel kan tillämpas på sådan civil underrättelseinhämtning och användning av metoder för underrättelseinhämtning som avses i 1 mom.

40 §

Beräkning av tidsfrister vid civil underrättelseinhämtning

Vid beräkning av tidsfrister enligt detta kapitel ska inte lagen om beräknande av laga tid (150/1930) tillämpas.

En i månader uttryckt tid löper ut den dag i månaden som till sitt ordningsnummer motsvarar den dag då tidsfristen började löpa. Om motsvarande dag inte finns i den månad då tidsfristen löper ut, löper tiden ut den sista dagen i månaden.

41 §

Förbud mot avlyssning och observation vid civil underrättelseinhämtning

Teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation får inte riktas mot sådan kommunikation som parterna i kommunikat-

ionen inte får vittna om eller som parterna har rätt att vägra vittna om med stöd av 17 kap. 13, 14, 16, 20 § eller 22 § 2 mom. i rättegångsbalken.

Om det under tiden för teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation eller vid något annat tillfälle framkommer att det är fråga om ett meddelande som det är förbjudet att avlyssna eller observera, ska åtgärden avbrytas och de upptagningar som fåtts genom åtgärden och anteckningarna om de uppgifter som fåtts genom den genast utplånas.

De förbud mot avlyssning och observation som avses i denna paragraf gäller dock inte sådana fall där en i 1 mom. avsedd person deltar i sådan verksamhet som är föremål för civil underrättelseinhämtning där verksamheten allvarligt hotar den nationella säkerheten och det även för hans eller hennes del har fattats beslut om teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation.

42 §

Granskning av upptagningar och handlingar från civil underrättelseinhämtning

En polisman som hör till befälet vid skyddspolisen eller en av denne förordnad tjänsteman ska utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av en metod för civil underrättelseinhämtning.

43 §

Undersökning av upptagningar från civil underrättelseinhämtning

Upptagningar som uppkommit vid användningen av metoder för civil underrättelseinhämtning får undersökas endast av domstol och en polisman som hör till befälet vid skyddspolisen. Enligt förordnande av en polisman som hör till befälet vid skyddspolisen eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en expert eller av någon annan som anlitas för inhämtande av information.

44 §

Utlämnande av information som erhållits vid civil underrättelseinhämtning för brottsbekämpning

Skyddspolisen ska utan ogrundat dröjsmål anmäla till centralkriminalpolisen, om det medan en metod för underrättelseinhämtning används framkommer att det kan antas att ett sådant brott har begåtts för vilket det föreskrivna strängaste straffet är fängelse i minst sex år. Genom beslut av chefen för skyddspolisen får anmälan skjutas upp med högst ett år åt gången, om det är nödvändigt för att garantera den nationella säkerheten eller skydda liv eller hälsa. Skyddspolisen får anmäla ett begånget brott till centralkriminalpolisen, om det föreskrivna strängaste straffet för brottet är fängelse i minst tre år.

Skyddspolisen ska utan dröjsmål anmäla till en behörig myndighet, om det medan en metod för underrättelseinhämtning används framkommer att ett sådant brott är på färde för vilket det föreskrivna strängaste straffet är fängelse i minst sex år och brottet ännu kan förhindras. Information som fåtts genom användning av en metod för underrättelseinhämtning får lämnas ut till en behörig myndighet för förhindrande av ett sådant brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år.

När det övervägs om en anmälan ska skjutas upp enligt 1 mom. eller en anmälan göras enligt 1 eller 2 mom. i fråga om ett begånget brott för vilket det föreskrivna strängaste straffet är fängelse i minst tre år eller i fråga om förhindrade av ett brott för vilket det föreskrivna sträng-

aste straffet är fängelse i minst två år, ska betydelsen av utredningen eller förhindrandet av brottet med tanke på allmänna och enskilda intressen beaktas vid bedömningen.

Information som fåtts genom användning av en metod för underrättelseinhämtning får alltid lämnas ut som utredning som stöder det att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada.

Om en förundersökningsmyndighet inleder en förundersökning eller börjar vidta en förundersökningsåtgärd eller en behörig myndighet inleder en åtgärd som syftar till att förhindra ett brott utifrån en anmälan som avses i denna paragraf, ska förundersökningsmyndigheten eller den behöriga myndigheten innan förundersökningen inleds, förundersökningsåtgärden vidtas eller den brottsförhindrande åtgärden vidtas anmäla detta till skyddspolisen.

45 §

Utplåning av information som erhållits vid en metod för underrättelseinhämtning

Information som fåtts genom en metod för underrättelseinhämtning ska utplånas utan dröjsmål efter att det framgått att den inte behövs för att skydda den nationella säkerheten.

Informationen får dock bevaras och lagras i ett register som avses i lagen om behandling av personuppgifter i polisens verksamhet, om detta behövs i fall som avses i 44 §.

Basstationsuppgifter som avses i 7 § ska utplånas efter att det har framgått att de inte behövs för att skydda den nationella säkerheten.

46 §

Utplåning av information som fåtts i en brådskande situation

Om en polisman som hör till befälet vid skyddspolisen i en brådskande situation enligt 7 § 1 mom., 8 § 1 mom., 11 § 1 mom., 12 § 1 mom., 13 § 1 mom., 14 § 1 mom. eller 27 § 2 mom. har beslutat att teleövervakning, inhämtande av basstationsuppgifter, teknisk avlyssning, optisk observation, teknisk spårning av en person, teknisk observation av utrustning eller platsspecifik underrättelseinhämtning ska inledas, men domstolen anser att det inte har funnits förutsättningar för åtgärden, ska användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Information som fåtts på detta sätt får dock användas under samma förutsättningar som en uppgift får användas i de fall som avses i 44 § 1 eller 2 mom., om det kan antas att det har begåtts ett sådant brott för vilket det strängaste föreskrivna straffet är fängelse i minst sex år eller om det framgår att ett sådant brott är på färde för vilket det strängaste föreskrivna straffet är fängelse i minst sex år och brottet ännu kan förhindras.

Om en polisman vid skyddspolisen i en brådskande situation enligt 33 § 2 mom. har beslutat om kopiering, men en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning anser att det inte har funnits förutsättningar för åtgärden, ska användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Information som fåtts på detta sätt får dock användas under samma förutsättningar som en uppgift får användas i de fall som avses i 44 § 1 eller 2 mom., om det kan antas att det har begåtts ett sådant brott för vilket det strängaste föreskrivna straffet är fängelse i minst sex år eller om det framgår att ett sådant brott är på färde för vilket det strängaste föreskrivna straffet är fängelse i minst sex år och brottet ännu kan förhindras.

47 §

Underrättelse om användning av metod för underrättelseinhämtning

Den person som vid civil underrättelseinhämtning har varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning och teknisk observation samt kopiering som riktar sig mot ett meddelande eller sådan kopiering av en försändelse som riktar sig mot ett meddelande ska utan dröjsmål underrättas om detta skriftligen efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts. Den som varit föremål för inhämtande av information ska dock underrättas om användningen av metoden för underrättelseinhämtning senast ett år från det att användningen av metoden upphörde.

På yrkande av en polisman som hör till befälet vid skyddspolisen får domstolen besluta att underrättelsen enligt 1 mom. till den som varit föremål för åtgärden får skjutas upp med högst två år åt gången, om det är motiverat för att trygga pågående användning av en metod för underrättelseinhämtning, garantera den nationella säkerheten eller skydda liv eller hälsa. Domstolen får besluta att underrättelsen ska utebli, om det är nödvändigt för att garantera den nationella säkerheten eller skydda liv eller hälsa.

Om den som varit föremål för inhämtandet av information inte är identifierad vid utgången av den tid eller det uppskov som avses i 1 eller 2 mom., ska han eller hon utan ogrundat dröjsmål skriftligen underrättas om underrättelseinhämtningen när identiteten har utretts.

Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om underrättelsen.

Om skyddspolisen fortsätter inhämtandet av information med stöd av 5 §, ska bestämmelserna om underrättelse om hemligt inhämtande av information i 5 kap. 58 § iakttas.

Den som vid civil underrättelseinhämtning varit föremål för inhämtande av information behöver inte underrättas om systematisk observation, förtäckt inhämtande av information, en täckoperation, bevisprovokation genom köp, styrd användning av informationskällor, platsspecifik underrättelseinhämtning, kopiering som riktar sig mot annat än ett meddelande och sådan kopiering av en försändelse som riktar sig mot annat än ett meddelande, om inte förundersökning har inletts i ärendet utifrån en anmälan enligt 44 §. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen iakttas.

Den som varit föremål för inhämtande av information behöver inte underrättas om användningen av en metod för underrättelseinhämtning, om föremålet har varit en statlig aktör eller en aktör som är jämställbar med en sådan.

I fråga om handläggning av underrättelseärenden i domstol ska 35 § iakttas.

48 §

Protokoll

Efter det att användningen av en metod för underrättelseinhämtning upphört ska det utan ogrundat dröjsmål upprättas ett protokoll över användningen av metoden.

49 §

Begränsning av partsoffentlighet i vissa fall

En person vars rättigheter eller skyldigheter saken gäller har inte, trots 11 § i lagen om offentlighet i myndigheternas verksamhet (621/1999), rätt att få vetskap om användningen av en sådan metod för underrättelseinhämtning som avses i detta kapitel förrän en underrättelse enligt 47 § har gjorts.

Bestämmelser om rätt till insyn för registrerade finns i lagen om behandling av personuppgifter i polisens verksamhet.

50 §

Rätt att få information av privata sammanslutningar

Trots att en sammanslutnings medlemmar, revisorer, verkställande direktör, styrelsemedlemmar eller arbetstagare är bundna av företags-, bank- eller försäkringshemlighet har skyddspolisen på begäran av en polisman som hör till befälet vid skyddspolisen rätt att få uppgifter som i ett enskilt fall kan antas vara behövliga vid utredningen av sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten och som kan antas vara av betydelse för att

1) identifiera eller nå en fysisk eller juridisk person som är föremål för civil underrättelseinhämtning, eller klarlägga personens kontaktuppgifter eller hur personen förflyttar sig,

2) inrikta användningen av en metod för underrättelseinhämtning på en viss person som är föremål för civil underrättelseinhämtning, eller

3) klarlägga ekonomisk verksamhet som antas anknyta till i 3 § avsedd verksamhet som bedrivs av en person eller en juridisk person som är föremål för civil underrättelseinhämtning.

51 §

Teleföretags skyldighet att biträda civil underrättelseinhämtning

På teleföretags skyldighet att biträda vid civil underrättelseinhämtning tillämpas vad som i 5 kap. 61 § föreskrivs om teleföretags skyldighet att biträda.

52 §

Ersättningar till teleföretag för biträde och lämnande av uppgifter vid civil underrättelseinhämtning

På teleföretags rätt till ersättning för direkta kostnader som orsakats av att de biträtt myndigheter och lämnat uppgifter vid civil underrättelseinhämtning tillämpas bestämmelserna i 5 kap. 62 §.

53 §

Användning av uppgifter som lagras av teleföretag och hänför sig till civil underrättelseinhämtning

Utöver vad som i 157 § 1 mom. i lagen om tjänster inom elektronisk kommunikation föreskrivs om användning av lagrade uppgifter får lagrade uppgifter som hänför sig till civil underrättelseinhämtning också användas om uppgifterna med fog kan antas vara av synnerlig vikt för att få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten.

54 §

Samarbete med militärunderrättelsemyndigheterna

Skyddspolisen ska samarbeta med militärunderrättelsemyndigheterna för att den civila och militära underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt och i detta syfte, trots det som föreskrivs om sekretess, ge militärunderrättelsemyndigheterna behövliga uppgifter.

55 §

Samarbete med andra myndigheter och sammanslutningar

Skyddspolisen ska enligt behov agera i samarbete med andra myndigheter för att den civila underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt.

Skyddspolisen får för att genomföra sitt uppdrag avseende civil underrättelseinhämtning agera i samarbete med sammanslutningar samt till andra myndigheter och sammanslutningar trots sekretessbestämmelserna lämna ut uppgifter, om utlämnandet av uppgifterna är nödvändigt för att skydda den nationella säkerheten.

Bestämmelser om utlämnande av information för brottsbekämpning finns i 44 §.

56 §

Samordning av hemlig informationsinhämtning

Användningen av de metoder för underrättelseinhämtning om vilka det föreskrivs i detta kapitel ska vid behov samordnas för att säkerställa arbetssäkerheten för skyddspolisens, militärunderrättelsemyndigheternas, centralkriminalpolisens och andra myndigheters tjänstemän samt för att förhindra att de taktiska och tekniska metoder och planer som nämnda myndigheter använder vid hemlig informationsinhämtning avslöjas.

57 §

Internationellt samarbete

Skyddspolisen får samarbeta och inhämta information tillsammans med utländska säkerhets- och underrättelsetjänster för att skydda den nationella säkerheten.

Om gemensam informationsinhämtning genomförs i samarbete med den stat, på vars territorium metoder för underrättelseinhämtning är avsedda att användas, ska en polisman vid skyddspolisen iaktta de begränsningar och villkor för användningen av metoderna för underrättelseinhämtning som staten i fråga ställer.

Chefen för skyddspolisen beslutar om deltagande i internationellt samarbete och om användning av metoder för underrättelseinhämtning i samband med det. En främmande stats behöriga tjänsteman har genom beslut av chefen för skyddspolisen rätt att på finskt territorium för att skydda den nationella säkerheten agera i samarbete med skyddspolisen, och under uppsikt och övervakning av en polisman vid skyddspolisen använda sådana metoder för underrättelseinhämtning om vars användning beslut fattas i enlighet med 9, 10, 18, 20 och 24 §.

Skyddspolisen får vid internationellt samarbete, trots sekretessbestämmelserna, lämna ut information, om utlämnandet av informationen behövs för att skydda den nationella säkerheten och utlämnandet inte strider mot ett nationellt intresse.

Bestämmelser om utlämnande av personuppgifter finns i lagen om behandling av personuppgifter i polisens verksamhet.

58 §

Samordning av underrättelseverksamheten

Den civila och den militära underrättelseverksamheten samordnas mellan republikens president, statsrådets kansli, utrikesministeriet, försvarsministeriet och inrikesministeriet samt vid behov andra ministerier och myndigheter.

Om det bedöms att den civila underrättelseverksamheten har utrikes- och säkerhetspolitiska konsekvenser, ska ärendet förberedelsevis behandlas mellan de myndigheter som avses i 1 mom.

59 §

Inrikesförvaltningens övervakning av den civila underrättelseinhämtningen

Det inhämtande av information som avses i detta kapitel övervakas av chefen för skyddspolisen och av inrikesministeriet.

60 §

Extern övervakning av den civila underrättelseinhämtningen

Inrikesministeriet ska årligen till riksdagens justitieombudsman och underrättelseombudsmannen lämna en berättelse om hur de i detta kapitel avsedda metoderna för underrättelseinhämtning har använts och användningen övervakats samt hur det i detta kapitel avsedda skyddandet av den civila underrättelseinhämtningen har använts och användningen övervakats.

Bestämmelser om den övervakning som underrättelseombudsmannen utövar finns i lagen om övervakning av underrättelseverksamheten (/).

61 §

Anmälningar till underrättelseombudsmannen

Skyddspolisen ska informera underrättelseombudsmannen om de tillstånd och beslut som gäller användning av en metod för underrättelseinhämtning och som har meddelats med stöd av detta kapitel så snart som möjligt efter det att tillståndet beviljades eller beslutet fattades.

Skyddspolisen ska så snart som möjligt informera underrättelseombudsmannen om ett beslut som gäller

1) skyddande av civil underrättelseverksamhet,

2) yppandeförbud,

3) uppskjutande av en anmälan enligt 44 § 1 mom.

Vid underrättelse om ett beslut som gäller en metod för underrättelseinhämtning ska det fästas särskild vikt vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.

62 §

Bemyndigande att utfärda förordning

Genom förordning av statsrådet får det utfärdas bestämmelser om

1) hur användningen av metoder för underrättelseinhämtning och skyddandet av dem ska ordnas,

2) dokumenteringen av åtgärderna för övervakningen,

3) de redogörelser som ska lämnas för övervakningen av den civila underrättelseinhämtningen,

4) förfarandet vid överföring av uppgifter som ska lämnas ut för brottsbekämpning,

5) hur samarbetet mellan skyddspolisen och militärunderrättelsemyndigheterna ska ordnas,

6) hur samarbetet mellan skyddspolisen och andra myndigheter ska ordnas,

7) hur samordningen av den hemliga informationsinhämtningen ska ordnas,

8) hur samordningen av underrättelseverksamheten ska ordnas.

Genom förordning av inrikesministeriet får det utfärdas bestämmelser om
1) hur övervakningen av den civila underrättelseverksamheten ska ordnas inom inrikesförvaltningen,
2) hur samarbetet mellan skyddspolisen och den övriga inrikesförvaltningen ska ordnas,
3) hur skyddspolisens internationella samarbete ska ordnas.

9 kap.

Särskilda bestämmelser

10 §

Närmare bestämmelser

— —

Genom förordning av inrikesministeriet kan närmare bestämmelser utfärdas om
1) hur polismäns ställning ska anges och polismän identifieras,
2) förvaring av egendom som tagits om hand,
3) polisundersökning,
4) tecken och metoder vid stoppande av fordon,
5) automatisk övervakning av vägtrafiken,
6) definitioner av användningen av maktmedel, utbildning i användningen av maktmedel, träning i och uppföljning av användningen av maktmedel, rätt att bära maktmedelsredskap, förvaring av maktmedelsredskap och övervakning av användningen av maktmedel,
7) fasttagande, förvaring och avlivande av djur,
8) handräckning till andra än Tullen och Gränsbevakningsväsendet,
9) registrering av polisåtgärder,
10) tekniskt utförande av säkerhetskontrollåtgärder, hur säkerhetskontroller ska ordnas i praktiken och om ordnande av säkerhetskontrollutbildning,
11) uniformsmodeller och märken som ska användas med uniform samt om när tjänsteuppgifterna är av sådan art eller karaktär att de förutsätter användning av uniform.

———

Denna lag träder i kraft den 20 .

———

2.

Lag

om civil underrättelseinhämtning avseende datatrafik

I enlighet med riksdagens beslut föreskrivs:

1 §

Tillämpningsområde och förhållande till annan lagstiftning

Denna lag innehåller bestämmelser om användning av underrättelseinhämtning som avser datatrafik vid sådan civil underrättelseinhämtning som avses i 5 a kap. i polislagen (872/2011).

Bestämmelser om användningen av underrättelseinhämtning som avser datatrafik vid militär underrättelseinhämtning och det tekniska genomförandet av underrättelseinhämtning som avser datatrafik finns i lagen om militär underrättelseverksamhet (/). Bestämmelser om teleavlyssning, inhämtande av information i stället för teleavlyssning och teleövervakning vid civil underrättelseinhämtning finns i 5 a kap. i polislagen.

Till den del det inte i denna lag föreskrivs om behandlingen av de uppgifter som erhållits vid underrättelseinhämtning som avser datatrafik, finns det bestämmelser om behandlingen av uppgifterna i lagen om behandling av personuppgifter i polisens verksamhet (761/2003).

2 §

Definitioner

I denna lag avses med

1) *underrättelseinhämtning som avser datatrafik* teknisk informationsinhämtning riktad mot datatrafik i kommunikationsnät som överskrider Finlands gräns, vilken baserar sig på automatiserad avskiljning av datatrafiken, samt behandling av den inhämtade informationen,

2) *kommunikationsnät* ett system som består av sammankopplade ledningar och av anordningar och som är avsett för överföring eller distribution av meddelanden via ledning, med radiovågor, optiskt eller på något annat elektromagnetiskt sätt,

3) *dataöverförare* den som äger eller innehar den del av ett kommunikationsnät som överskrider Finlands gräns.

3 §

Föremål för underrättelseinhämtning som avser datatrafik

Genom underrättelseinhämtning som avser datatrafik får information inhämtas om

1) terrorism,

2) utländsk underrättelseverksamhet,

3) planering, tillverkning, spridning och användning av massförstörelsevapen,

4) planering, tillverkning, spridning och användning av sådana produkter med dubbel användning som avses i 2 § i lagen om kontroll av export av produkter med dubbel användning (562/1996),

5) verksamhet som hotar den demokratiska samhällsordningen,

6) verksamhet som hotar ett stort antal människors liv eller hälsa eller samhällets vitala funktioner,

7) en främmande stats verksamhet som kan orsaka skada för Finlands internationella relationer, ekonomiska intressen eller andra viktiga intressen,
8) en kris som hotar internationell fred och säkerhet,
9) verksamhet som hotar säkerheten vid internationella krishanteringsinsatser,
10) verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och deltar i annan internationell verksamhet,
11) internationell organiserad brottslighet som hotar samhällsordningen.

4 §

Förutsättningar för användning av underrättelseinhämtning som avser datatrafik

En allmän förutsättning för användning av underrättelseinhämtning som avser datatrafik är att det med fog kan antas att man genom den kan få information om sådan verksamhet som är föremål för underrättelseinhämtning som avser datatrafik och som allvarligt hotar den nationella säkerheten.

Om användningen av sökbegreppen vid underrättelseinhämtning som avser datatrafik inte gäller enbart en statlig aktörs eller med en sådan jämställbar aktörs datatrafik, är en ytterligare förutsättning att den underrättelseinhämtning som avser datatrafik kan antas vara nödvändig för att få information om sådan verksamhet som är föremål för underrättelseinhämtning som avser datatrafik och som allvarligt hotar den nationella säkerheten.

5 §

Inriktande av underrättelseinhämtning som avser datatrafik

Inriktandet av underrättelseinhämtning som avser datatrafik genomförs med hjälp av automatiserad avskiljning av datatrafiken. Den automatiserade avskiljningen baserar sig på användningen av sådana sökbegrepp som godkänts i ett förfarande enligt 7 eller 9 §.

Ett sökbegrepp som beskriver innehållet i ett meddelande får användas endast om
1) sökbegreppet används endast i fråga om en främmande stats eller med en sådan jämställbar aktörs datatrafik, eller
2) sökbegreppet beskriver innehållet i ett skadligt datorprogram eller skadligt datakommando.

Som sökbegrepp får inte användas uppgifter som identifierar terminalutrustning eller en teleadress som innehas av eller annars förmodligen används av en person som befinner sig i Finland.

6 §

Fortsatt behandling av information som samlats in med hjälp av automatiserad avskiljning

Den datatrafik som avskilts automatiserat på det sätt som avses i 5 § får behandlas automatiskt och manuellt. Vid behandlingen får innehållet i meddelanden och andra konfidentiella uppgifter utredas.

7 §

Tillstånd av domstol för underrättelseinhämtning som avser datatrafik

Beslut om underrättelseinhämtning som avser datatrafik fattas av domstol på skriftligt yrkande av chefen för skyddspolisen.

I ett yrkande och i ett beslut om underrättelseinhämtning som avser datatrafik ska följande nämnas:

1) den verksamhet enligt 3 § som är föremål för underrättelseinhämtningen,

2) fakta om den verksamhet som avses i 1 punkten,

3) de fakta som ligger till grund för förutsättningarna för användningen av underrättelseinhämtning som avser datatrafik,

4) de sökbegrepp eller kategorier av sökbegrepp som ska användas i underrättelseinhämtningen samt motiveringarna till dem,

5) den del av ett kommunikationsnät som överskrider Finlands gräns där sökbegreppen i fråga om den datatrafik som rör sig där används samt motiveringarna till valet av kommunikationsnätsdel,

6) giltighetstiden med angivande av klockslag för tillståndet till underrättelseinhämtning som avser datatrafik,

7) den för uppdraget förordnade, till befälet vid skyddspolisen hörande polisman som är förtrogen med användningen av metoder för underrättelseinhämtning och som leder och övervakar genomförandet av underrättelseinhämtningen,

8) eventuella begränsningar och villkor för underrättelseinhämtningen.

Tillstånd till underrättelseinhämtning som avser datatrafik får beviljas för högst sex månader åt gången.

Underrättelseinhämtning som avser datatrafik ska avslutas före utgången av den tid som anges i beslutet, om syftet med underrättelseinhämtningen har nåtts eller om det inte längre finns förutsättningar för den.

8 §

Förfarandet i domstol

Vid handläggning och avgörande i domstol av tillståndsärenden som gäller underrättelseinhämtning som avser datatrafik ska de bestämmelser i 5 a kap. 35 § i polislagen som gäller handläggningen av tillståndsärenden som gäller metoder för underrättelseinhämtning iakttas.

9 §

Beslutsförfarande i brådskande situationer

Om ett ärende som gäller underrättelseinhämtning som avser datatrafik inte tål uppskov, får chefen för skyddspolisen besluta om underrättelseinhämtning som avser datatrafik till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Beslutet ska fattas skriftligen. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att underrättelseinhämtningen inleddes.

Om domstolen anser att det inte funnits förutsättningar i enlighet med 4 § för underrättelseinhämtning som avser datatrafik, ska användningen av underrättelseinhämtningen omedelbart avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Om domstolen anser att det beslut som avses i 1 mom. till någon annan del har varit felaktigt ska användningen av underrättelseinhämtningen omedelbart avslutas till den del som detta förutsätts i domstolens avgörande, samt det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt till samma delar utplånas utan dröjsmål. Informationen får dock bevaras och lagras i ett register som avses i lagen om behandling av personuppgifter i polisens verksamhet under de förutsättningar som anges i 5 a kap. 46 § 1 mom. i polislagen.

10 §

Tekniskt genomförande av underrättelseinhämtning som avser datatrafik och annat samarbete med militärunderrättelsemyndigheten

Försvarsmaktens underrättelsetjänst är teknisk utförare av underrättelseinhämtning som avser datatrafik.

Skyddspolisen kan ge Försvarsmaktens underrättelsetjänst i uppdrag att behandla tekniska data i enlighet med 63 § i lagen om militär underrättelseverksamhet. Försvarsmaktens underrättelsetjänst ansöker för skyddspolisens räkning om tillstånd enligt 64 § i lagen om militär underrättelseverksamhet att behandla tekniska data samt lämnar resultatet av en sådan statistisk analys som avses i 63 § 2 mom. i den lagen till skyddspolisen efter det att underrättelsetjänsten har fått tillstånd till behandlingen av tekniska data och utfört åtgärderna i enlighet med tillståndet.

Skyddspolisen lämnar det beslut som avses i 7 eller 9 § till Försvarsmaktens underrättelsetjänst, som utför de uppgifter som avses i 5 § för skyddspolisens räkning. Försvarsmaktens underrättelsetjänst lämnar den datatrafik som underrättelsetjänsten har avskilt i enlighet med uppdraget till skyddspolisen.

På skyddspolisens övriga samarbete med militärunderrättelsemyndigheterna tillämpas 5 a kap. 54 § i polislagen.

11 §

Beräkning av tidsfrister

Vid beräkning av tidsfrister enligt denna lag ska inte lagen om beräknande av laga tid (150/1930) tillämpas.

En i månader uttryckt tid löper ut den dag i månaden som till sitt ordningsnummer motsvarar den dag då tidsfristen började löpa. Om motsvarande dag inte finns i den månad då tidsfristen löper ut, löper tiden ut den sista dagen i månaden.

12 §

Förbud mot underrättelseinhämtning

Underrättelseinhämtning som avser datatrafik får inte riktas mot ett meddelande vars avsändare och mottagare befinner sig i Finland eller mot sådana uppgifter som avsändaren, mottagaren eller den som lagrat informationen har skyldighet eller rätt att vägra vittna med stöd av 17 kap. 13, 14, 16 eller 20 § eller 22 § 2 mom. i rättegångsbalken.

13 §

Granskning av upptagningar och handlingar

En i 5 kap. 7 § i polislagen avsedd polisman som hör till befälet vid skyddspolisen eller en av denne förordnad tjänsteman ska utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av underrättelseinhämtning som avser datatrafik.

14 §

Undersökning av upptagningar

Upptagningar som uppkommit vid användningen av underrättelseinhämtning som avser datatrafik får undersökas endast av domstol och en polisman som hör till befälet vid skyddspolisen. Enligt förordnande av en polisman som hör till befälet vid skyddspolisen eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en expert eller av någon annan som anlitas för inhämtande av information.

15 §

Utplåning av information

Information som fåtts genom underrättelseinhämtning som avser datatrafik ska utplånas utan dröjsmål om det framgår att

1) båda parterna i kommunikationen befann sig i Finland när kommunikationen försiggick,

2) avsändaren, mottagaren eller den som lagrat informationen har skyldighet eller rätt att vägra vittna om informationen på det sätt som avses i 12 §,

3) informationen inte behövs för att skydda den nationella säkerheten.

Information som avses i 1 mom. 3 punkten får dock lämnas ut för brottsbekämpning under de förutsättningar som anges i 5 a kap. 44 § i polislagen samt bevaras och lagras i ett register som avses i lagen om behandling av personuppgifter i polisens verksamhet under de förutsättningar som anges i 5 a kap. 45 § 1 mom. i polislagen.

För utplåningen av informationen svarar den tekniska utföraren av underrättelseinhämtning som avser datatrafik, eller uppdragsgivaren i det fall att informationen redan har lämnats till uppdragsgivaren.

16 §

Utlämnande av information om skadliga datorprogram eller skadliga datakommandon till myndigheterna, företag eller sammanslutningar

Skyddspolisen får trots sekretessbestämmelserna lämna ut sådan information som inhämtats med hjälp av underrättelseinhämtning som avser datatrafik och som gäller skadliga datorprogram eller skadliga datakommandon till myndigheter, företag eller sammanslutningar, om utlämnandet av informationen behövs för att skydda den nationella säkerheten eller informationsmottagarens intressen.

På tystnadsplikten för den som är anställd av ett företag eller en sammanslutning tillämpas bestämmelserna i 23 § 2 mom. i lagen om offentlighet i myndigheternas verksamhet (621/1999).

17 §

Utlämnande av information för brottsbekämpning

På utlämnade av information som erhållits genom underrättelseinhämtning som avser datatrafik för brottsbekämpning tillämpas bestämmelserna i 5 a kap. 44 § i polislagen.

18 §

Begränsning av partsoffentlighet i vissa fall

Trots det som föreskrivs i 11 § i lagen om offentlighet i myndigheternas verksamhet har en person inte rätt att få vetskap om användningen av underrättelseinhämtning som avser datatrafik förrän en underrättelse enligt 20 § har gjorts.

Bestämmelser om rätt till insyn för registrerade finns i lagen om behandling av personuppgifter i polisens verksamhet.

19 §

Protokoll

Efter det att användningen av underrättelseinhämtning som avser datatrafik upphört ska skyddspolisen utan ogrundat dröjsmål upprätta ett protokoll.

20 §

Underrättelse om underrättelseinhämtning som avser datatrafik

Om det vid sådan behandling som avses i 6 § manuellt har klarlagts innehållet i ett förtroligt meddelande som en person som befinner sig i Finland har sänt eller tagit emot eller i information som en sådan person har lagrat, ska personen underrättas om den underrättelseinhämtning som avser datatrafik med iakttagande av vad som i 5 a kap. 47 § i polislagen föreskrivs om underrättelse om teleavlyssning. Skyldighet att underrätta om underrättelseinhämtning som avser datatrafik föreligger emellertid inte, om informationen har utplånats med stöd av 9 § 2 mom. eller 15 §.

21 §

Genomförande av den koppling som underrättelseinhämtning som avser datatrafik förutsätter

Vid genomförande av den koppling som underrättelseinhämtning som avser datatrafik förutsätter vid civil underrättelseinhämtning iakttas bestämmelserna i 72 § i lagen om militär underrättelseverksamhet.

22 §

Dataöverförares skyldighet att lämna uppgifter

En dataöverförare ska utan obefogat dröjsmål, på en specificerad begäran av en för uppdraget förordnad sådan till befälet hörande polisman vid skyddspolisen som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning, lämna skyddspolisen de tekniska data som dataöverföraren förfogar över beträffande uppbyggnaden av ett kommunikationsnät som överskrider Finlands gräns och dirigeringen av datatrafiken i det, när dessa tekniska data behövs för att identifiera en del av ett kommunikationsnät för ett sådant yrkande om tillstånd eller tillståndsbeslut för användning av underrättelseinhämtning som avser datatrafik som ska föreläggas domstolen.

23 §

Ersättningar till dataöverförare

En dataöverförare har rätt att få ersättning av statens medel för direkta kostnader som orsakats av att överföraren har lämnat uppgifter enligt 22 §. Beslut om betalning av ersättning fattas av skyddspolisen.

Omprövning av beslutet får begäras på det sätt som anges i förvaltningslagen (434/2003). Det beslut som meddelas med anledning av begäran om omprövning får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996). Över förvaltningsdomstolens beslut får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

24 §

Inrikesförvaltningens övervakning av underrättelseinhämtning som avser datatrafik

Det inhämtande av information som avses i denna lag övervakas av chefen för skyddspolisen och av inrikesministeriet.

25 §

Extern övervakning av underrättelseinhämtning som avser datatrafik

Inrikesministeriet ska årligen till riksdagens justitieombudsman och underrättelseombudsmannen lämna en berättelse om användningen av den underrättelseinhämtning som avser datatrafik.

Bestämmelser om den övervakning som underrättelseombudsmannen utövar finns i lagen om övervakning av underrättelseverksamheten (/).

26 §

Anmälningar till underrättelseombudsmannen

Skyddspolisen ska informera underrättelseombudsmannen om de tillstånd och beslut som domstolen har meddelat med stöd av denna lag så snart som möjligt efter det att de har meddelats.

27 §

Befogenhet att utfärda förordning

Närmare bestämmelser om ordnandet och övervakningen av användningen av underrättelseinhämtning som avser datatrafik samt om dokumentering av åtgärderna och om de redogörelser som ska lämnas för övervakningen får utfärdas genom förordning av statsrådet.

28 §

Ikraftträdande

Denna lag träder i kraft den 20 .

———

3.

Lag

om ändring av 10 och 15 a § i polisförvaltningslagen

I enlighet med riksdagens beslut
ändras i polisförvaltningslagen (110/1992) 10 § 1 och 2 mom.,
sådana de lyder i lag 860/2015, och
fogas till 15 a §, sådan den lyder i lagarna 873/2011, 1165/2013 och 421/2017, ett nytt 3 mom., i stället för det 3 mom. som upphävts genom lag 1165/2013, som följer:

10 §

Skyddspolisen

Skyddspolisen har till uppgift att i enlighet med inrikesministeriets styrning inhämta information för att skydda den nationella säkerheten samt upptäcka, förhindra och avslöja sådan verksamhet, sådana förehavanden och sådana brott som kan hota statsskicket och samhällsordningen eller rikets inre eller yttre säkerhet. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att upptäcka och förhindra verksamhet som hotar samhällets säkerhet.

Inrikesministeriet bestämmer, efter att ha hört Polisstyrelsen, vid behov närmare om samverkan och samarbetet mellan skyddspolisen och andra polisenheter.

— —

15 a §

Polisbefogenheter

— —

Utöver det som föreskrivs i 1 mom. har en tjänsteman vid skyddspolisen rätt att använda i 5 a kap. i polislagen avsedda metoder för underrättelseinhämtning för att skydda den nationella säkerheten i enlighet med vad som föreskrivs i det kapitlet.

———

Denna lag träder i kraft den 20 .

———

4.

Lag

om ändring av lagen om behandling av personuppgifter i polisens verksamhet

I enlighet med riksdagens beslut

ändras i lagen om behandling av personuppgifter i polisens verksamhet (761/2003) 5 § 2 mom., 13 § 1 mom. 2, 4, 6, 15 och 16 punkten och 45 § 1 mom. 5 punkten,

av dem 13 § 1 mom. 2 punkten sådan den lyder i lag 1073/2015, 13 § 4 och 6 punkten sådana de lyder i lag 457/2009 och 13 § 15 och 16 punkten sådana de lyder i lag 29/2015 samt 45 § 1 mom. 5 punkten sådan den lyder i lag 1181/2013, som följer:

5 §

Skyddspolisens funktionella informationssystem

— —

Skyddspolisens funktionella informationssystem kan innehålla uppgifter som skyddspolisen måste behandla för att kunna skydda den nationella säkerheten eller för att kunna förhindra, avslöja eller utreda förehavanden eller brott som äventyrar rätts- och samhällsordningen eller statens säkerhet.

— —

13 §

Polisens rätt att få uppgifter ur vissa register och informationssystem

Utöver vad som föreskrivs i någon annan lag har polisen trots sekretessbestämmelserna rätt att i enlighet med vad som avtalas om saken med den registeransvarige i fråga ur vissa register genom en teknisk anslutning eller som en datamängd få sådan information som polisen behöver för att utföra sina uppdrag och föra sina personregister, enligt följande:

— —

2) uppgifter som gäller dömda, fångar eller intagna i en enhet vid Brottspåföljdsmyndigheten ur Brottspåföljdsmyndighetens informationssystem som avses i 14 § 1 och 2 mom. i lagen om behandling av personuppgifter vid Brottspåföljdmyndigheten (1069/2015) för skyddande av den nationella säkerheten, för förhindrande, avslöjande, utredning av brott och överlämnande av brott till åtalsprövning och för ett sådant tillstånd eller godkännande från polisen som förutsätter att personen i fråga är tillförlitlig,

— —

4) av dem som utövar inkvarteringsverksamhet sådana uppgifter om resande som avses i 6 § 1 mom. i lagen om inkvarterings- och förplägnadsverksamhet (308/2006) och som behövs för att skydda den nationella säkerheten, upprätthålla allmän ordning och säkerhet samt för att förhindra, avslöja eller utreda brott och för att utföra något annat för polisen lagstadgat uppdrag,

— —

6) ur Patent- och registerstyrelsens handelsregister, för skyddande av den nationella säkerheten och för förhindrande, avslöjande och utredande av brott, uppgifter om anmälningar och meddelanden som gäller näringsidkare,

— —

15) ur det register över laddare som avses i 3 § i lagen om laddare (219/2000) uppgifter för övervaknings- och larmuppdrag samt för skyddande av den nationella säkerheten och för förhindrande, utredning och avslöjande av brott,

16) av samfund och sammanslutningar uppgifter ur register som gäller passagerare och fordons personal, för skyddande av den nationella säkerheten, för förhindrande, avslöjande och utredning av brott och överlämnande av brott till åtalsprövning samt för att nå efterlysta personer.

— —

45 §

Inskränkningar i rätten till insyn

Rätten till insyn gäller inte

— —

5) uppgifter som erhållits vid utövande av befogenheterna enligt 4 kap. 3 § eller 5 eller 5 a kap. i polislagen, befogenheterna enligt 10 kap. i tvångsmedelslagen eller befogenheterna enligt lagen om civil underrättelseinhämtning avseende datatrafik (/),

— —

———

Denna lag träder i kraft den 20 .

———

5.

Lag

om ändring av 2 kap. 1 § i förundersökningslagen

I enlighet med riksdagens beslut
ändras i förundersökningslagen (805/2011) 2 kap. 1 § 1 mom. som följer:

2 kap.

Vilka som deltar i förundersökning

1 §

Myndigheterna vid förundersökning

Förundersökning görs av någon annan polis än skyddspolisen.

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av 12 kap. i strafflagen

I enlighet med riksdagens beslut
fogas till 12 kap. i strafflagen (39/1889) en ny 12 § som följer:

12 kap.

Om landsförräderibrott

12 §

Begränsningsbestämmelse

Såsom brott som avses i detta kapitel anses inte sådan användning av metoder för underrättelseinhämtning som avses i 5 a kap. i polislagen (872/2011), i lagen om civil underrättelseinhämtning avseende datatrafik (/) eller i lagen om militär underrättelseverksamhet (/).

Denna lag träder i kraft den 20 .

7.

Lag

om ändring av 2 och 10 kap. i tvångsmedelslagen

I enlighet med riksdagens beslut

ändras i tvångsmedelslagen (806/2011) 2 kap. 9 § samt 10 kap. 3 § 1 mom., 6 § 1 mom. och 39 § 1 mom., av dem 2 kap. 9 § sådan den lyder delvis ändrad i lag 1146/2013, som följer:

2 kap.

Gripande, anhållande och häktning

9 §

Anhållningsberättigade tjänstemän

En anhållningsberättigad tjänsteman beslutar om anhållande. Anhållningsberättigade tjänstemän är

1) polisöverdirektören, vid Polisstyrelsen polisdirektörer, polisöverinspektörer och polisinspektörer, polischefer, biträdande polischefer, vid centralkriminalpolisen chefen för centralkriminalpolisen och biträdande chefer, kriminalöverinspektörer, kriminalinspektörer, kriminalöverkommissarier, överkommissarier, kriminalkommissarier och kommissarier,

2) Tullens brottsbekämpningschef, chefen för verksamhetsenheten för Tullens brottsbekämpning och de tullöverinspektörer vid Tullens brottsbekämpning som av Tullens brottsbekämpningschef har förordnats till undersökningsledare,

3) chefen och biträdande chefen för Gränsbevakningsväsendet, avdelningschefen för gräns- och sjöavdelningen vid staben för Gränsbevakningsväsendet, avdelningschefen, biträdande avdelningschefen, enhetschefen vid enheten för brottsbekämpning, överinspektörerna för gränsbevakningsfrågor, överinspektörerna, kriminalöverinspektörerna och kriminalinspektörerna på juridiska avdelningen vid staben för Gränsbevakningsväsendet, kommendörerna och biträdande kommendörerna för gränsbevaknings- och sjöbevakningssektionerna, chefen för en gränsbyrå eller sjöbyrå vid en gränsbevaknings- eller sjöbevakningssektion, chefen och biträdande chefen för Helsingfors gränskontrollavdelning vid Finska vikens sjöbevakningssektion och en sådan gränsbevakningsman med minst löjtnants grad som genomgått den utbildning som föreskrivs för undersökningsledare inom Gränsbevakningsväsendet och som av chefen för Gränsbevakningsväsendet eller chefen för någon av dess förvaltningsenheter har förordnats till undersökningsledare,

4) åklagare.

I fråga om anhållningsberättigade tjänstemän vid försvarsmakten föreskrivs särskilt.

10 kap.

Hemliga tvångsmedel

3 §

Teleavlyssning och dess förutsättningar

Med *teleavlyssning* avses att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett i 3 § 43 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) avsett allmänt kommunikationsnät eller ett därtill anslutet

kommunikationsnät avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 6 §. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en person som är misstänkt för brott.

— —

6 §

Teleövervakning och dess förutsättningar

Med *teleövervakning* avses att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät som avses i 3 § eller som har mottagits till en sådan adress eller utrustning samt att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att användningen av adressen eller utrustningen tillfälligt förhindras. Med *identifieringsuppgifter* avses sådana uppgifter om ett meddelande som kan förknippas med en i 3 § 7 punkten i lagen om tjänster inom elektronisk kommunikation avsedd användare eller med en i 30 punkten i den paragrafen avsedd abonnent och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.

— —

39 §

Användning av informationskällor och förutsättningar för styrd användning av informationskällor

Med *användning av informationskällor* avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av i 1 kap. 1 § avsedda uppgifter av personer som inte hör till polisen eller till någon annan myndighet (*informationskälla*).

— —

———

Denna lag träder i kraft den 20 .

———

8.

Lag

om ändring av lagen om offentlighet vid rättegång i allmänna domstolar

I enlighet med riksdagens beslut

ändras i lagen om offentlighet vid rättegång i allmänna domstolar (370/2007) 5 § 1 och 2 mom., 12 § 2 mom. och 16 § 4 mom.,

sådana de lyder, 5 § 2 mom. och 16 § 4 mom. i lag 1159/2013 och 12 § 2 mom. i lagarna 821/2011, 633/2015 och 13/2016, och

fogas till 5 § ett nytt 3 mom., till 12 § 2 mom. en ny 3 a-punkt och till 16 § ett nytt 5 mom. som följer:

5 §

Tidpunkten för när de grundläggande uppgifterna om en rättegång blir offentliga

De grundläggande uppgifter om rättegången som avses i 4 § blir genast offentliga, om inte något annat följer av 2 och 3 mom.

I ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen (806/2011), 5 kap. i polislagen (872/2011) eller 3 kap. i lagen om brottsbekämpning inom Tullen (623/2015) eller som gäller en metod för underrättelseinhämtning enligt 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik (/) eller lagen om militär underrättelseverksamhet (/) och i vilket den som är föremål för metoden inte behöver höras vid behandlingen av yrkandet på metoden, blir de grundläggande uppgifterna offentliga först när den som misstänks för brott eller är föremål för metoden senast ska underrättas om att sådana metoder använts. Om personen i fråga underrättas om användningen av metoden senare därför att hans eller hennes identitet inte har varit känd, blir de grundläggande uppgifterna offentliga när domstolen informeras om underrättelsen. Domstolen får besluta att de grundläggande uppgifterna ska bli offentliga tidigare.

I ett ärende som gäller ett i 15 § i lagen om övervakning av underrättelseverksamheten (/) avsett interimistiskt förordnande av underrättelseombudsmannen tillämpas i fråga om tidpunkten för när uppgifterna blir offentliga bestämmelserna i 2 mom.

12 §

En parts rätt att ta del av en handling

— —

En parts rätt enligt 1 mom. gäller inte

1) information som avses i 11 § 2 mom. 7 och 7 a-punkten i lagen om offentlighet i myndigheternas verksamhet,

2) rättegångshandlingar som upprättats vid en domstol, före den tidpunkt som avses i 8 §,

3) ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen, 5 kap. i polislagen eller 3 kap. i lagen om brottsbekämpning inom Tullen eller som gäller en metod för underrättelseinhämtning enligt 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik eller lagen om militär underrättelseverksamhet och i vilket den som är föremål för metoden inte behöver höras vid behandlingen av yrkandet på metoden,

3 a) ett ärende som gäller ett i 15 § i lagen om övervakning av underrättelseverksamheten avsett interimistiskt förordnande av underrättelseombudsmannen, eller

4) rättegångshandlingar till den del de innehåller uppgifter om domstolens överläggning.

16 §

Offentligheten i tvångsmedelsärenden

— —

Ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen, 5 kap. i polislagen eller 3 kap. i lagen om brottsbekämpning inom Tullen eller som gäller en metod för underrättelseinhämtning enligt 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik eller lagen om militär underrättelseverksamhet och i vilket den som är föremål för metoden inte behöver höras vid behandlingen av yrkandet på metoden, handläggs och avgörandet avkunnas utan att allmänheten är närvarande. Den rättegångshandling som innehåller avgörandet samt övriga rättegångshandlingar i ärendet blir offentliga när den som misstänks för brott eller är föremål för metoden senast ska underrättas om att metoden använts. Om personen i fråga underrättas om användningen av metoden senare när hans eller hennes identitet är utredd, blir rättegångshandlingarna offentliga när domstolen informeras om underrättelsen. Domstolen får av särskilda skäl besluta att en rättegångshandling ska bli offentlig tidigare.

Ett ärende som gäller ett i 15 § i lagen om övervakning av underrättelseverksamheten avsett interimistiskt förordnande av underrättelseombudsmannen handläggs och avgörandet avkunnas utan att allmänheten är närvarande. I fråga om tidpunkten för när den rättegångshandling som innehåller avgörandet samt övriga rättegångshandlingar i ärendet blir offentliga tillämpas 4 mom.

———

Denna lag träder i kraft den 20 .

———

Helsingfors den 25 januari 2018

Statsminister

Juha Sipilä

Inrikesminister Paula Risikko

Parallelltext

1.

Lag

om ändring av polislagen

I enlighet med riksdagens beslut

ändras i polislagen (872/2011) 1 kap. 1 § 1 mom., 5 kap. 5 § 1 mom., 7 § 1 och 3 mom., 8 § 1 mom., 10 § 1–4 mom. och 6 mom., 12 § 1 och 3 mom., 14 § 1 och 3 mom., 16 § 1 mom., 18 § 2 och 4 mom., 20 § 1, 2 och 4 mom., 22 § 1, 2 och 4 mom., 24 § 1 och 3 mom., 25 § 3 mom., 32 § 1 mom., 36 § 1 och 3 mom., 38 § 1 mom., 39 § 1 mom., 40 § 1 mom., 42 § 1 mom., 44 § 1 mom., 47 § 2 mom., 48 § 1 mom., 52 och 57 §, 58 § 1 mom., 61 § 2 mom. och den finska språkdräkten i 63 § 2 mom., den finska språkdräkten i 9 kap. 8 § och 9 § 2 mom. samt 9 kap. 10 § 2 mom.,

av dem 5 kap. 7 § 3 mom., 10 § 3 och 6 mom., 12 § 3 mom., 18 § 4 mom., 20 § 4 mom., 22 § 4 mom., 47 § 2 mom. och 58 § 1 mom. sådana de lyder i lag 1168/2013, och

fogas till lagen ett nytt 5 a kap. som följer:

Gällande lydelse	*Föreslagen lydelse*
1 kap	**1 kap.**
Allmänna bestämmelser	**Allmänna bestämmelser**
1 §	1 §
Polisens uppgifter	*Polisens uppgifter*
Polisens uppgift är att trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning. Polisen ska upprätthålla säkerheten i samarbete med andra myndigheter samt med sammanslutningar och invånarna och sköta det internationella samarbete som hör till dess uppgifter.	Polisens uppgift är att trygga rätts- och samhällsordningen, *skydda den nationella säkerheten,* upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning. Polisen ska upprätthålla säkerheten i samarbete med andra myndigheter samt med sammanslutningar och invånarna och sköta det internationella samarbete som hör till dess uppgifter.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Gällande lydelse	*Föreslagen lydelse*
5 kap.	**5 kap.**
Hemliga metoder för inhämtande av information	**Hemliga metoder för inhämtande av information**
5 §	5 §
Teleavlyssning och dess förutsättningar	*Teleavlyssning och dess förutsättningar*
Med teleavlyssning avses att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett sådant allmänt kommunikationsnät eller ett *sådant* därtill anslutet kommunikationsnät som avses i kommunikationsmarknadslagen (393/2003) avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 8 §. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas göra sig skyldig till ett brott som avses i 2 mom.	Med *teleavlyssning* avses att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom *ett i 3 § 43 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) avsett* allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 8 §. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas göra sig skyldig till ett brott som avses i 2 mom.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
7 §	7 §
Beslut om teleavlyssning och motsvarande inhämtande av information	*Beslut om teleavlyssning och motsvarande inhämtande av information*
På yrkande av en polisman som avses i 2 kap. 9 § 1 mom. 1 punkten i tvångsmedelslagen (anhållningsberättigad polisman) beslutar domstolen om teleavlyssning och inhämtande av information i stället för teleavlyssning.	*Beslut* om teleavlyssning och inhämtande av information i stället för teleavlyssning *ska fattas av domstol* på yrkande av en polisman som avses i 2 kap. 9 § 1 mom. 1 punkten i tvångsmedelslagen (*anhållningsberättigad polisman*) *eller på yrkande av chefen eller en biträdande chef för skyddspolisen eller en avdelningschef, överinspektör eller inspektör vid skyddspolisen* (*polisman som hör till befälet vid skyddspolisen*).
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I ett yrkande och i ett beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,	I ett yrkande och i ett beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,

Gällande lydelse	*Föreslagen lydelse*
3) de fakta som misstanken mot personen och förutsättningarna för teleavlyssningen eller för inhämtandet av information i stället för teleavlyssning grundar sig på,	3) de fakta som misstanken mot personen och förutsättningarna för teleavlyssningen eller för inhämtandet av information i stället för teleavlyssning grundar sig på,
4) giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning eller inhämtande av information enligt 6 § 2 mom.,	4) giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning eller inhämtande av information enligt 6 § 2 mom.,
5) den teleadress eller teleterminalutrustning som åtgärden riktas mot,	5) den teleadress eller teleterminalutrustning som åtgärden riktas mot,
6) den *anhållningsberättigade* polisman som leder och övervakar utförandet av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning,	6) den *i 1 mom. avsedda* polisman som leder och övervakar utförandet av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning,
7) eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.	7) eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.
8 §	8 §
Teleövervakning och dess förutsättningar	*Teleövervakning och dess förutsättningar*
Med *teleövervakning* avses att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät som avses i 5 § eller som har mottagits till en sådan adress eller utrustning samt att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att användningen av adressen eller utrustningen tillfälligt förhindras. Med *identifieringsuppgifter* avses i 2 § 8 punkten i lagen om dataskydd vid elektronisk kommunikation (516/2004) avsedda uppgifter om ett meddelande vilka kan förknippas med en abonnent eller användare och behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.	Med *teleövervakning* avses att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät som avses i 5 § eller som har mottagits till en sådan adress eller utrustning samt att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att användningen av adressen eller utrustningen tillfälligt förhindras. Med *identifieringsuppgifter* avses *sådana* uppgifter om ett meddelande *som* kan förknippas med en *i 3 § 7* punkten i lagen om *tjänster inom elektronisk kommunikation avsedd användare eller med en i 30 punkten i den paragrafen avsedd abonnent och som* behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
10 §	10 §
Beslut om teleövervakning	*Beslut om teleövervakning*
På yrkande av en anhållningsberättigad polisman ska domstolen besluta om teleövervakning enligt 8 § 2 och 5 mom. samt 9 § 1, 4 och 5 punkten och om teleövervakning i de fall som avses i 3 §.	*Beslut* om teleövervakning enligt 8 § 2 och 5 mom. samt 9 § 1, 4 och 5 punkten och om teleövervakning i de fall som avses i 3 § ska *fattas av* domstol på yrkande av en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen.*

Gällande lydelse	*Föreslagen lydelse*
Om ett ärende som gäller annan i 1 mom. avsedd teleövervakning än sådan som avses i 3 § inte tål uppskov, får en anhållningsberättigad polisman besluta om teleövervakning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.	Om ett ärende som gäller annan i 1 mom. avsedd teleövervakning än sådan som avses i 3 § inte tål uppskov, får en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* besluta om teleövervakning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.
Chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning ska besluta om teleövervakning som avses i 8 § 4 mom. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman besluta om teleövervakningen till dess att chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning har avgjort ärendet om teleövervakning. Ärendet ska föras till nämnda polisman för avgörande så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.	Chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning ska besluta om teleövervakning som avses i 8 § 4 mom. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* besluta om teleövervakningen till dess att chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning har avgjort ärendet om teleövervakning. Ärendet ska föras till nämnda polisman för avgörande så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.
En anhållningsberättigad polisman ska besluta om teleövervakning som avses i 8 § 3 mom. och 9 § 2 och 3 punkten.	En anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* ska besluta om teleövervakning som avses i 8 § 3 mom. och 9 § 2 och 3 punkten.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I ett yrkande och i ett beslut om teleövervakning ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för teleövervakning grundar sig på, 4) samtycke, om detta är ett villkor för teleövervakningen, 5) tillståndets giltighetstid med angivande av klockslag, 6) den teleadress eller teleterminalutrustning som åtgärden riktas mot, 7) den *anhållningsberättigade* polisman som leder och övervakar utförandet av teleövervakningen, 8) eventuella begränsningar och villkor för teleövervakningen.	I ett yrkande och i ett beslut om teleövervakning ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för teleövervakning grundar sig på, 4) samtycke, om detta är ett villkor för teleövervakningen, 5) tillståndets giltighetstid med angivande av klockslag, 6) den teleadress eller teleterminalutrustning som åtgärden riktas mot, 7) den polisman som leder och övervakar utförandet av teleövervakningen *och som avses i 7 § 1 mom.*, 8) eventuella begränsningar och villkor för teleövervakningen.

Gällande lydelse	*Föreslagen lydelse*
12 §	12 §
Beslut om inhämtande av basstationsuppgifter	*Beslut om inhämtande av basstationsuppgifter*
Beslut om inhämtande av basstationsuppgifter ska fattas av domstolen på yrkande av en anhållningsberättigad polisman. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman besluta om inhämtande av basstationsuppgifter till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.	Beslut om inhämtande av basstationsuppgifter ska fattas av domstol på yrkande av en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen*. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* besluta om inhämtande av basstationsuppgifter till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart *det är* möjligt, dock senast 24 timmar efter det att metoden började användas.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I ett yrkande och i ett beslut om inhämtande av basstationsuppgifter ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) de fakta som ligger till grund för förutsättningarna för inhämtande av basstationsuppgifter, 3) den tidsperiod som tillståndet gäller, 4) vilken basstation tillståndet gäller, 5) den *anhållningsberättigade* polisman som leder och övervakar inhämtandet av basstationsuppgifter, 6) eventuella begränsningar och villkor för inhämtandet av basstationsuppgifter.	I ett yrkande och i ett beslut om inhämtande av basstationsuppgifter ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) de fakta som ligger till grund för förutsättningarna för inhämtande av basstationsuppgifter, 3) den tidsperiod som tillståndet gäller, 4) vilken basstation tillståndet gäller, 5) den polisman som leder och övervakar inhämtandet av basstationsuppgifter *och som avses i 7 § 1 mom.,* 6) eventuella begränsningar och villkor för inhämtandet av basstationsuppgifter.
14 §	14 §
Beslut om systematisk observation	*Beslut om systematisk observation*
Beslut om systematisk observation ska fatttas av en anhållningsberättigad polisman.	Beslut om systematisk observation ska fatttas av en anhållningsberättigad polisman *eller av en polisman som hör till befälet vid skyddspolisen.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Beslut om systematisk observation ska fatttas skriftligen. I beslutet ska följande nämnas: 1) det brott som ligger till grund för åtgärden samt brottstidpunkten,	Beslut om systematisk observation ska fatttas skriftligen. I beslutet ska följande nämnas: 1) det brott som ligger till grund för åtgärden samt brottstidpunkten,

Gällande lydelse	*Föreslagen lydelse*
2) den person som med fog kan antas begå det brott som avses i 1 punkten,	2) den person som med fog kan antas begå det brott som avses i 1 punkten,
3) de fakta för misstanken mot personen och den systematiska observationen grundar sig på,	3) de fakta som misstanken mot personen och den systematiska observationen grundar sig på,
4) tillståndets giltighetstid,	4) tillståndets giltighetstid,
5) den *anhållningsberättigade* polisman som leder och övervakar genomförandet av den systematiska observationen,	5) den polisman som leder och övervakar genomförandet av den systematiska observationen *och som avses i 7 § 1 mom.*,
6) eventuella begränsningar och villkor för den systematiska observationen.	6) eventuella begränsningar och villkor för den systematiska observationen.
16 §	16 §
Beslut om förtäckt inhämtande av information	*Beslut om förtäckt inhämtande av information*
Beslut om förtäckt inhämtande av information ska fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen, chefen för en polisinrättning eller en för uppdraget förordnad anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information.	Beslut om förtäckt inhämtande av information ska fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen *eller* chefen för en polisinrättning eller av en för uppdraget förordnad *sådan* anhållningsberättigad polisman *eller polisman som hör till befälet vid skyddspolisen* som särskilt utbildats för hemligt inhämtande av information.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
18 §	18 §
Beslut om teknisk avlyssning	*Beslut om teknisk avlyssning*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Beslut om teknisk avlyssning som avses i 17 § 5 mom. och om annan än i 1 mom. avsedd teknisk avlyssning ska fattas av en anhållningsberättigad polisman.	Beslut om teknisk avlyssning som avses i 17 § 5 mom. och om annan än i 1 mom. avsedd teknisk avlyssning ska fattas av en anhållningsberättigad polisman *eller av en polisman som hör till befälet vid skyddspolisen*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I ett yrkande och i ett beslut om teknisk avlyssning ska följande nämnas:	I ett yrkande och i ett beslut om teknisk avlyssning ska följande nämnas:
1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden,	1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden,
2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,	2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten,
3) de fakta som misstanken mot personen och förutsättningarna för den tekniska avlyssningen grundar sig på,	3) de fakta som misstanken mot personen och förutsättningarna för den tekniska avlyssningen grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,	4) tillståndets giltighetstid med angivande av klockslag,

Gällande lydelse	*Föreslagen lydelse*
5) det utrymme eller den plats av annat slag som avlyssningen riktas mot, 6) den *anhållningsberättigade* polisman som leder och övervakar genomförandet av den tekniska avlyssningen, 7) eventuella begränsningar och villkor för den tekniska avlyssningen.	5) det utrymme eller den plats av annat slag som avlyssningen riktas mot, 6) den polisman som leder och övervakar genomförandet av den tekniska avlyssningen *och som avses i 7 § 1 mom*., 7) eventuella begränsningar och villkor för den tekniska avlyssningen.
20 §	20 §
Beslut om optisk observation	*Beslut om optisk observation*
Beslut om optisk observation ska fattas av domstolen på yrkande av en anhållningsberättigad polisman, om observationen riktas mot ett hemfridsskyddat utrymme eller en annan plats som avses i 24 kap. 11 § i strafflagen eller mot en person som berövats sin frihet på grund av brott. Beslut om optisk observation som avses i 19 § 5 mom. och om annan än i 1 mom. avsedd optisk observation ska fattas av en anhållningsberättigad polisman.	Beslut om optisk observation ska fattas av domstol på yrkande av en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen*, om observationen riktas mot ett sådant hemfridsskyddat utrymme eller en annan plats som avses i 24 kap. 11 § i strafflagen eller mot en person som berövats sin frihet på grund av brott. Beslut om optisk observation som avses i 19 § 5 mom. och om annan än i 1 mom. avsedd optisk observation ska fattas av en anhållningsberättigad polisman *eller av en polisman som hör till befälet vid skyddspolisen.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I ett yrkande och i ett beslut om optisk observation ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för den optiska observationen grundar sig på, 4) tillståndets giltighetstid med angivande av klockslag, 5) det utrymme eller den plats av annat slag som observationen riktas mot, 6) den a*nhållningsberättigade* polisman som leder och övervakar genomförandet av den optiska observationen, 7) eventuella begränsningar och villkor för den optiska observationen.	I ett yrkande och i ett beslut om optisk observation ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för den optiska observationen grundar sig på, 4) tillståndets giltighetstid med angivande av klockslag, 5) det utrymme eller den plats av annat slag som observationen riktas mot, 6) den polisman som leder och övervakar genomförandet av den optiska observationen *och som avses i 7 § 1 mom*., 7) eventuella begränsningar och villkor för den optiska observationen.

Gällande lydelse	*Föreslagen lydelse*
22 §	22 §
Beslut om teknisk spårning	*Beslut om teknisk spårning*
Beslut om teknisk spårning av en person ska fattas av domstolen på yrkande av en anhållningsberättigad polisman. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman besluta om sådan spårning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.	Beslut om teknisk spårning av en person ska fattas av domstol på yrkande av en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen*. Om ärendet inte tål uppskov, får en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* besluta om sådan spårning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart *det är* möjligt, dock senast 24 timmar efter det att metoden började användas.
En anhållningsberättigad polisman ska besluta om teknisk spårning som avses i 21 § 4 mom. och om annan än i 1 mom. avsedd teknisk spårning.	*Beslut* om teknisk spårning som avses i 21 § 4 mom. och om annan än i 1 mom. avsedd teknisk spårning *ska fattas av* en anhållningsberättigad polisman *eller av en polisman som hör till befälet vid skyddspolisen*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I ett yrkande och i ett beslut om teknisk spårning ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för den tekniska spårningen grundar sig på, 4) tillståndets giltighetstid med angivande av klockslag, 5) det föremål, det ämne eller den egendom som spårningen riktas mot, 6) den *anhållningsberättigade* polisman som leder och övervakar genomförandet av den tekniska spårningen, 7) eventuella begränsningar och villkor för den tekniska spårningen.	I ett yrkande och i ett beslut om teknisk spårning ska följande nämnas: 1) det brott som ligger till grund för åtgärden och den förmodade brottstidpunkten eller den fara som ligger till grund för åtgärden, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för den tekniska spårningen grundar sig på, 4) tillståndets giltighetstid med angivande av klockslag, 5) det föremål, det ämne eller den egendom som spårningen riktas mot, 6) den polisman som leder och övervakar genomförandet av den tekniska spårningen *och som avses i 7 § 1 mom.*, 7) eventuella begränsningar och villkor för den tekniska spårningen.
24 §	24 §
Beslut om teknisk observation av utrustning	*Beslut om teknisk observation av utrustning*
Beslut om teknisk observation av utrustning ska fattas av domstolen på yrkande av en anhållningsberättigad polisman. Om ärendet inte tål uppskov, får en anhållningsberätt-	Beslut om teknisk observation av utrustning ska fattas av domstol på yrkande av en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen*.

Gällande lydelse	*Föreslagen lydelse*
tigad polisman besluta om teknisk observation av utrustning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att metoden började användas.	Om ärendet inte tål uppskov, får en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* besluta om teknisk observation av utrustning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart *det är* möjligt, dock senast 24 timmar efter det att metoden började användas.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I ett yrkande och i ett beslut om teknisk observation av utrustning ska följande nämnas: 1) det brott som ligger till grund för åtgärden samt brottstidpunkten, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för den tekniska observationen av utrustning grundar sig på, 4) tillståndets giltighetstid med angivande av klockslag, 5) den tekniska anordning eller programvara som åtgärden riktas mot, 6) den *anhållningsberättigade* polisman som leder och övervakar genomförandet av den tekniska observationen av utrustning, 7) eventuella begränsningar och villkor för den tekniska observationen av utrustning.	I ett yrkande och i ett beslut om teknisk observation av utrustning ska följande nämnas: 1) det brott som ligger till grund för åtgärden samt brottstidpunkten, 2) den person som med fog kan antas göra sig skyldig till det brott som avses i 1 punkten, 3) de fakta som misstanken mot personen och förutsättningarna för den tekniska observationen av utrustning grundar sig på, 4) tillståndets giltighetstid med angivande av klockslag, 5) den tekniska anordning eller programvara som åtgärden riktas mot, 6) den polisman som leder och övervakar genomförandet av den tekniska observationen av utrustning *och som avses i 7 § 1 mom.*, 7) eventuella begränsningar och villkor för den tekniska observationen av utrustning.
25 §	25 §
Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning	*Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Beslut om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning fattas av en anhållningsberättigad polisman.	Beslut om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning *ska* fattas av en anhållningsberättigad polisman *eller av en polisman som hör till befälet vid skyddspolisen*.
32 §	32 §
Beslut om en täckoperation	*Beslut om en täckoperation*
Beslut om en täckoperation ska fattas av chefen för centralkriminalpolisen eller chefen för skyddspolisen. Chefen för centralkriminalpolisen, chefen för skyddspolisen, chefen för polisinrättningen eller en för uppdraget	Beslut om en täckoperation ska fattas av chefen för centralkriminalpolisen eller chefen för skyddspolisen. *Beslut* om *en* täckoperation som genomförs uteslutande i datanät *får fattas också* av chefen för centralkriminalpo-

Gällande lydelse	*Föreslagen lydelse*
förordnad anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information ska besluta om täckoperationer som genomförs uteslutande i datanät.	lisen, chefen för skyddspolisen eller chefen för en polisinrättning eller av en för uppdraget förordnad *sådan* anhållningsberättigad polisman *eller polisman som hör till befälet vid skyddspolisen* som särskilt utbildats för hemligt inhämtande av information.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
36 §	36 §
Beslut om bevisprovokation genom köp	*Beslut om bevisprovokation genom köp*
Beslut om bevisprovokation genom köp ska fattas av chefen för centralkriminalpolisen eller chefen för skyddspolisen. Beslut om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten får fattas också av en för uppdraget förordnad anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information.	Beslut om bevisprovokation genom köp ska fattas av chefen för centralkriminalpolisen eller chefen för skyddspolisen. Beslut om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten får fattas också av en för uppdraget förordnad *sådan* anhållningsberättigad polisman *eller polisman som hör till befälet vid skyddspolisen* som särskilt utbildats för hemligt inhämtande av information.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Beslut om bevisprovokation genom köp ska fattas skriftligen. I beslutet ska följande nämnas: 1) det brott som ligger till grund för åtgärden, 2) den person som är föremål för bevisprovokationen, 3) de fakta som brottsmisstanken och förutsättningarna för bevisprovokationen grundar sig på, 4) de föremål, de ämnen, den egendom eller de tjänster som är föremål för bevisprovokationen, 5) syftet med bevisprovokationen, 6) tillståndets giltighetstid, 7) den anhållningsberättigade polisman som leder och övervakar genomförandet av bevisprovokationen, 8) eventuella begränsningar och villkor för bevisprovokationen.	Beslut om bevisprovokation genom köp ska fattas skriftligen. I beslutet ska följande nämnas: 1) det brott som ligger till grund för åtgärden, 2) den person som är föremål för bevisprovokationen, 3) de fakta som brottsmisstanken och förutsättningarna för bevisprovokationen grundar sig på, 4) de föremål, de ämnen, den egendom eller de tjänster som är föremål för bevisprovokationen, 5) syftet med bevisprovokationen, 6) *beslutets* giltighetstid, 7) den anhållningsberättigade polisman *eller till befälet vid skyddspolisen hörande polisman* som leder och övervakar genomförandet av bevisprovokationen, 8) eventuella begränsningar och villkor för bevisprovokationen.
38 §	38 §
Beslut om genomförande av bevisprovokation genom köp	*Beslut om genomförande av bevisprovokation genom köp*
Beslut om genomförande av bevisprovo-	Beslut om genomförande av bevisprovo-

Gällande lydelse	*Föreslagen lydelse*
kation genom köp ska fattas skriftligen. Beslutet ska fattas av en anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information och som ansvarar för genomförandet av bevisprovokationen.	kation genom köp ska fattas skriftligen. Beslutet ska fattas av en sådan anhållningsberättigad polisman *eller polisman som hör till befälet vid skyddspolisen* som särskilt utbildats för hemligt inhämtande av information och som ansvarar för genomförandet av bevisprovokationen.
39 §	39 §
Säkerheten för en polisman vid förtäckt inhämtande av information, en täckoperation och vid bevisprovokation genom köp	*Säkerheten för en polisman vid förtäckt inhämtande av information, en täckoperation och vid bevisprovokation genom köp*
En anhållningsberättigad polisman får besluta att en polisman som ska genomföra förtäckt inhämtande av information, en täckoperation eller bevisprovokation genom köp ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att polismannens säkerhet ska kunna tryggas.	En anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* får besluta att en polisman som ska genomföra förtäckt inhämtande av information, en täckoperation eller bevisprovokation genom köp ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att polismannens säkerhet ska kunna tryggas.
40 §	40 §
Användning av informationskällor och förutsättningar för styrd användning av informationskällor	*Användning av informationskällor och förutsättningar för styrd användning av informationskällor*
Med *användning av informationskällor* avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av i 1 kap. 1 § avsedda uppgifter av personer som inte hör till polisen eller till någon annan *förundersöknings*myndighet *(informationskälla)*.	Med *användning av informationskällor* avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av i 1 kap. 1 § avsedda uppgifter av personer som inte hör till polisen eller till någon annan myndighet (*informationskälla*).
42 §	42 §
Beslut om styrd användning av informationskällor	*Beslut om styrd användning av informationskällor*
Beslut om styrd användning av informationskällor ska fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen, chefen för en polisinrättning eller av en för uppdraget förordnad anhållningsberätti-	Beslut om styrd användning av informationskällor ska fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen eller chefen för en polisinrättning eller av en för uppdraget förordnad sådan anhåll-

Gällande lydelse	*Föreslagen lydelse*
gad polisman som särskilt utbildats för hemligt inhämtande av information.	ningsberättigad polisman *eller polisman som hör till befälet vid skyddspolisen* som särskilt utbildats för hemligt inhämtande av information.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
44 §	44 §
Beslut om kontrollerade leveranser	*Beslut om kontrollerade leveranser*
Beslut om kontrollerade leveranser som utförs av polisen fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen, chefen för en polisinrättning eller av en för uppdraget förordnad anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information. Det föreskrivs särskilt om andra myndigheters beslutsfattande om kontrollerade leveranser.	Beslut om kontrollerade leveranser som utförs av polisen ska fattas av chefen för centralkriminalpolisen, chefen för skyddspolisen *eller* chefen för en polisinrättning eller av en för uppdraget förordnad *sådan* anhållningsberättigad polisman *eller polisman som hör till befälet vid skyddspolisen* som särskilt utbildats för hemligt inhämtande av information. Det föreskrivs särskilt om andra myndigheters beslutsfattande om kontrollerade leveranser.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
47 §	47 §
Beslut om skyddande	*Beslut om skyddande*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
En anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information beslutar om annat än i 1 mom. avsett skyddande av inhämtande av information.	En sådan anhållningsberättigad polisman *eller polisman som hör till befälet vid skyddspolisen* som särskilt utbildats för hemligt inhämtande av information beslutar om annat än i 1 mom. avsett skyddande av inhämtande av information.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
48 §	48 §
Yppandeförbud som gäller hemligt inhämtande av information	*Yppandeförbud som gäller hemligt inhämtande av information*
En anhållningsberättigad polisman får av viktiga skäl som hänför sig till förhindrande eller avslöjande av brott förbjuda en utomstående att röja sådana omständigheter om användningen av hemligt inhämtande av information som denne fått kännedom om. Det förutsätts dessutom att den utomstående med anledning av sitt uppdrag eller sin ställning har bistått eller blivit ombedd att bistå vid hemligt inhämtande av information.	En anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* får av viktiga skäl som hänför sig till förhindrande eller avslöjande av brott förbjuda en utomstående att röja sådana omständigheter om användningen av hemligt inhämtande av information som denne fått kännedom om. Det förutsätts dessutom att den utomstående med anledning av sitt uppdrag eller sin ställning har bistått eller blivit ombedd

Gällande lydelse	*Föreslagen lydelse*
	att bistå vid hemligt inhämtande av information.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
52 §	52 §
Undersökning av upptagningar	*Undersökning av upptagningar*
Upptagningar som uppkommit vid hemligt inhämtande av information får undersökas endast av domstol och en anhållningsberättigad polisman. Enligt förordnande av den anhållningsberättigade polismannen eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en expert eller av någon annan som anlitas för inhämtande av information.	Upptagningar som uppkommit vid hemligt inhämtande av information får undersökas endast av domstol och en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen*. Enligt förordnande av den anhållningsberättigade polismannen *eller den polisman som hör till befälet vid skyddspolisen* eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en expert eller av någon annan som anlitas för inhämtande av information.
57 §	57 §
Utplåning av information som fåtts i en brådskande situation	*Utplåning av information som erhållits i en brådskande situation*
Om en anhållningsberättigad polisman i en brådskande situation enligt 10 § 2 mom., 12 § 1 mom., 22 § 1 mom. eller 24 § 1 mom. har beslutat att teleövervakning, inhämtande av basstationsuppgifter, teknisk spårning av en person eller teknisk observation av utrustning ska inledas men domstolen anser att det inte har funnits förutsättningar för åtgärden, ska inhämtandet av information avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Information som fåtts på detta sätt får dock användas på samma villkor som överskottsinformation får användas enligt 54 §.	Om en anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* i en brådskande situation enligt 10 § 2 mom., 12 § 1 mom., 22 § 1 mom. eller 24 § 1 mom. har beslutat att teleövervakning, inhämtande av basstationsuppgifter, teknisk spårning av en person eller teknisk observation av utrustning ska inledas men domstolen anser att det inte har funnits förutsättningar för åtgärden, ska inhämtandet av information avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Information som fåtts på detta sätt får dock användas på samma villkor som överskottsinformation får användas enligt 54 §.
58 §	58 §
Underrättelse om hemligt inhämtande av information	*Underrättelse om hemligt inhämtande av information*
Den som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, *systematisk ob-*	Den som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk obser-

Gällande lydelse	*Föreslagen lydelse*
servation, förtäckt inhämtande av information, teknisk observation och kontrollerade leveranser ska utan dröjsmål underrättas om detta skriftligen efter det att syftet med inhämtandet av information har nåtts. Personen i fråga ska dock underrättas om det hemliga inhämtandet av information senast ett år efter att det har upphört.	vation och kontrollerade leveranser ska utan dröjsmål underrättas om detta skriftligen efter det att syftet med inhämtandet av information har nåtts. Personen i fråga ska dock underrättas om det hemliga inhämtandet av information senast ett år efter att det har upphört.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
61 §	61 §
Teleföretags skyldighet att biträda samt tillträde till vissa utrymmen	*Teleföretags skyldighet att biträda samt tillträde till vissa utrymmen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Polisen, den som utför åtgärden och den biträdande personalen har rätt att för att göra de kopplingar som behövs för teleavlyssning få tillträde också till andra utrymmen än de som är i teleföretagets besittning, dock inte till utrymmen som används för stadigvarande boende. En anhållningsberättigad polisman beslutar om åtgärden. Det föreskrivs särskilt om husrannsakan.	Polisen, den som utför åtgärden och den biträdande personalen har rätt att för att göra de kopplingar som behövs för teleavlyssning få tillträde också till andra utrymmen än de som är i teleföretagets besittning, dock inte till utrymmen som används för stadigvarande boende. En anhållningsberättigad polisman *eller en polisman som hör till befälet vid skyddspolisen* beslutar om åtgärden. Det föreskrivs särskilt om husrannsakan.
(ny)	5 a kap.
	Civil underrättelseinhämtning
	1 §
	Tillämpningsområde
	Detta kapitel innehåller bestämmelser om skyddspolisens inhämtande och nyttjande av information för att den nationella säkerheten ska kunna skyddas och den högsta statsledningens beslutsfattande stödjas samt för att andra myndigheter ska kunna utföra de lagstadgade uppgifter som hänför sig till den nationella säkerheten (civil underrättelseinhämtning).
(ny)	2 §
	Metoder för civil underrättelseinhämtning
	Metoder för civil underrättelseinhämtning är teleavlyssning, inhämtande av information

Gällande lydelse	*Föreslagen lydelse*
	i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, teknisk spårning, teknisk observation av utrustning, inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp och styrd användning av informationskällor. *Metoder för civil underrättelseinhämtning är även i detta kapitel avsedd platsspecifik underrättelseinhämtning och kopiering samt i detta kapitel avsett kvarhållande av en försändelse för kopiering och inhämtande av information från privata sammanslutningar.* *I detta kapitel föreskrivs om förutsättningarna för användning av de i 1 mom. avsedda metoderna för underrättelseinhämtning och av platsspecifik underrättelseinhämtning, kopiering, kvarhållande av en försändelse för kopiering och rätt att få information av privata sammanslutningar vid civil underrättelseinhämtning.* *Bestämmelser om underrättelseinhämtning som avser datatrafik som en metod för civil underrättelseinhämtning finns i lagen om civil underrättelseinhämtning avseende datatrafik (/).*
(ny)	3 § *Föremål för civil underrättelseinhämtning* *Genom civil underrättelseinhämtning får information inhämtas om* *1) terrorism,* *2) utländsk underrättelseverksamhet,* *3) planering, tillverkning, spridning och användning av massförstörelsevapen,* *4) planering, tillverkning, spridning och användning av sådana produkter med dubbel användning som avses i 2 § i lagen om kontroll av export av produkter med dubbel användning (562/1996),* *5) verksamhet som hotar den demokratiska samhällsordningen,* *6) verksamhet som hotar ett stort antal människors liv eller hälsa eller samhällets vitala funktioner,* *7) en främmande stats verksamhet som kan*

Gällande lydelse	*Föreslagen lydelse*
	orsaka skada för Finlands internationella relationer, ekonomiska intressen eller andra viktiga intressen, *8) en kris som hotar internationell fred och säkerhet,* *9) verksamhet som hotar säkerheten vid internationella krishanteringsinsatser,* *10) verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och deltar i annan internationell verksamhet,* *11) internationell organiserad brottslighet som hotar samhällsordningen.*
(ny)	4 § *Förutsättningar för användning av metoderna för underrättelseinhämtning* *En allmän förutsättning för användning av en metod för civil underrättelseinhämtning är att det med fog kan antas att man genom metoden kan få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten.* *Utöver vad som nedan föreskrivs om särskilda förutsättningar för användning av metoder för underrättelseinhämtning får teleavlyssning, inhämtande av information i stället för teleavlyssning, systematisk observation, teknisk avlyssning, optisk observation, teknisk spårning av personer, teknisk observation av utrustning, täckoperationer, bevisprovokation genom köp, styrd användning av informationskällor och platsspecifik underrättelseinhämtning användas inom civil underrättelseinhämtning endast om dessa metoder med fog kan antas vara av synnerlig vikt för att få information om sådan verksamhet som avses i 1 mom. För täckoperationer och bevisprovokation genom köp förutsätts dessutom att användningen av metoden är nödvändig. En förutsättning för täckoperationer är dessutom att inhämtandet av information måste anses vara behövligt på grund av att verksamheten är planmässig, organiserad eller yrkesmässig eller på grund av att det kan antas att den fortsätter eller upprepas.* *Om en metod för underrättelseinhämtning riktas mot en statlig aktör eller en aktör som*

Gällande lydelse	*Föreslagen lydelse*
	är jämställbar med en sådan, ska på förutsättningarna för användningen av metoderna för underrättelseinhämtning tillämpas bara det som föreskrivs i 1 mom. *Metoder för underrättelseinhämtning får inte riktas mot ett utrymme som används för stadigvarande boende. Täckoperationer och bevisprovokation genom köp får dock företas i en bostad om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden.* *Användningen av en metod för underrättelseinhämtning ska avslutas före utgången av den tid som anges i beslutet, om syftet med användningen har nåtts eller om det inte längre finns förutsättningar för att använda metoden.*
(ny)	5 § *Fortsatt inhämtande av information för förhindrande och avslöjande av vissa brott* *Om det vid civil underrättelseinhämtning, medan en metod för underrättelseinhämtning används, framkommer att en person med fog kan antas göra sig skyldig till ett brott som nämns i 5 kap. 3 § eller till högförräderi, grovt högförräderi eller olaglig militär verksamhet eller det kan antas att ett sådant brott har begåtts och det genom användning av metoden för underrättelseinhämtning inte längre kan antas att man får information om den verksamhet som allvarligt hotar den nationella säkerheten och som låg till grund för tillståndet eller beslutet, får skyddspolisen fortsätta att använda metoden som en hemlig metod för inhämtande av information i avsikt att förhindra och avslöja brott under giltighetstiden för det tillstånd som fattats med stöd av detta kapitel, dock högst i en månads tid. Då ska ärendet inom den nämnda tiden föras för avgörande till den myndighet som är behörig att fatta beslut om användning av den aktuella metoden för inhämtande av information.*

Gällande lydelse	*Föreslagen lydelse*
(ny)	6 §
	Beslut om teleavlyssning och motsvarande inhämtande av information vid civil underrättelseinhämtning
	Beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. *Tillstånd till teleavlyssning och till inhämtande av information i stället för teleavlyssning får ges för högst sex månader åt gången. När åtgärden gäller en person får tillstånd ges för högst tre månader åt gången.* *I ett yrkande och i ett beslut om teleavlyssning och inhämtande av information i stället för teleavlyssning ska följande nämnas:* *1) den verksamhet som avses i 3 §,* *2) den person, teleadress eller teleterminalutrustning som åtgärden riktas mot,* *3) de fakta som förutsättningarna för och inriktningen av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning grundar sig på,* *4) giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning och till inhämtande av information i stället för teleavlyssning,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar teleavlyssningen eller inhämtandet av information i stället för teleavlyssning,* *6) eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.*
(ny)	7 §
	Beslut om teleövervakning vid civil underrättelseinhämtning
	Beslut om teleövervakning vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ett ärende som gäller teleövervakning inte tål uppskov, får chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid

Gällande lydelse	*Föreslagen lydelse*
	skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om teleövervakning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas. *För inhämtande av uppgifter om verksamhet som är föremål för civil underrättelseinhämtning får skyddspolisen med samtycke av den som innehar en teleadress eller teleterminalutrustning rikta teleövervakning mot teleadressen eller teleterminalutrustningen.* *Chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om sådan teleövervakning som avses i 2 mom.* *Tillstånd får beviljas och beslut fattas för högst sex månader åt gången, och tillståndet eller beslutet får gälla även en viss tid före tillståndet beviljades eller beslutet fattades, vilken kan vara längre än sex månader.* *I ett yrkande och i ett beslut om teleövervakning ska följande nämnas:* *1) åtgärden, dess syfte samt den verksamhet som avses i 3 §,* *2) den person, teleadress eller teleterminalutrustning som åtgärden riktas mot,* *3) de fakta som förutsättningarna för och inriktningen av teleövervakningen grundar sig på,* *4) tillståndets giltighetstid med angivande av klockslag,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar teleöver-vakningen,* *6) eventuella begränsningar och villkor för teleövervakningen.*
(ny)	8 § *Beslut om inhämtande av basstationsuppgifter vid civil underrättelseinhämtning* *Beslut om inhämtande av basstationsuppgifter vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om*

Gällande lydelse	*Föreslagen lydelse*
	ärendet inte tål uppskov, får en polisman som hör till befälet vid skyddspolisen besluta om inhämtande av basstationsuppgifter till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas. *Tillstånd beviljas för en viss tidsperiod.* *I ett yrkande och i ett beslut om inhämtande av basstationsuppgifter ska följande nämnas:* *1) den verksamhet som avses i 3 §,* *2) vilken basstation tillståndet gäller,* *3) de fakta som förutsättningarna för och inriktningen av inhämtandet av basstationsuppgifter grundar sig på,* *4) den tidsperiod som tillståndet gäller,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar inhämtandet av basstationsuppgifter,* *6) eventuella begränsningar och villkor för inhämtandet av basstationsuppgifter.*
(ny)	9 § *Beslut om systematisk observation vid civil underrättelseinhämtning* *Beslut om systematisk observation vid civil underrättelseinhämtning ska fattas av en polisman som hör till befälet vid skyddspolisen.* *Beslut om systematisk observation får fattas för högst sex månader åt gången.* *Beslut om systematisk observation ska fattas skriftligen. I beslutet ska följande nämnas:* *1) den verksamhet som avses i 3 §,* *2) den person eller grupp av personer som åtgärden riktas mot,* *3) de fakta som förutsättningarna för och inriktningen av den systematiska observationen grundar sig på,* *4) tillståndets giltighetstid,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar utförandet av den systematiska observationen,* *6) eventuella begränsningar och villkor för den systematiska observationen.*

Gällande lydelse	*Föreslagen lydelse*
(ny)	10 §
	Beslut om förtäckt inhämtande av information vid civil underrättelseinhämtning
	Beslut om förtäckt inhämtande av information vid civil underrättelseinhämtning ska fattas av chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning. *Beslutet om förtäckt inhämtande av information ska fattas skriftligen. I beslutet ska följande nämnas:* *1) åtgärden och dess syfte tillräckligt specificerat,* *2) den verksamhet som avses i 3 §,* *3) den person eller grupp av personer som åtgärden riktas mot,* *4) de fakta som förutsättningarna för och inriktningen av det förtäckta inhämtandet av information grundar sig på,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar det förtäckta inhämtandet av information,* *6) den planerade tidpunkten för genomförandet av åtgärden,* *7) eventuella begränsningar och villkor för det förtäckta inhämtandet av information.* *Vid förändrade omständigheter ska beslutet vid behov ses över.* *Om åtgärden inte tål uppskov, behöver ett beslut som avses i 1 mom. inte upprättas i skriftlig form före det förtäckta inhämtandet av information. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter det att åtgärden har vidtagits.*
(ny)	11 §
	Beslut om teknisk avlyssning vid civil underrättelseinhämtning
	Beslut om teknisk avlyssning som riktas mot en frihetsberövad person vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen

Gällande lydelse	*Föreslagen lydelse*
	och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om teknisk avlyssning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas. *En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om annan teknisk avlyssning än sådan som avses i 1 mom.* *Tillstånd får ges och beslut fattas för högst sex månader åt gången.* *I ett yrkande och i ett beslut om teknisk avlyssning ska följande nämnas:* *1) den verksamhet som avses i 3 §,* *2) den person eller grupp av personer eller det utrymme eller den plats av annat slag som åtgärden riktas mot,* *3) de fakta som förutsättningarna för och inriktningen av den tekniska avlyssningen grundar sig på,* *4) tillståndets giltighetstid med angivande av klockslag,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar den tekniska avlyssningen,* *6) eventuella begränsningar och villkor för den tekniska avlyssningen.*
(ny)	12 § *Beslut om optisk observation vid civil underrättelseinhämtning* *Beslut om optisk observation som riktas mot en frihetsberövad person vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om optisk observation till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.*

Gällande lydelse	*Föreslagen lydelse*
	En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning beslutar om annan optisk observation än sådan som avses i 1 mom. *Tillstånd får ges och beslut fattas för högst sex månader åt gången.* *I ett yrkande och i ett beslut om optisk observation ska följande nämnas:* *1) den verksamhet som avses i 3 §,* *2) den person eller grupp av personer eller det utrymme eller den plats av annat slag som åtgärden riktas mot,* *3) de fakta som förutsättningarna för och inriktningen av den optiska observationen grundar sig på,* *4) tillståndets giltighetstid med angivande av klockslag,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar den optiska observationen,* *6) eventuella begränsningar och villkor för den optiska observationen.*
(ny)	13 § *Beslut om teknisk spårning vid civil underrättelseinhämtning* *Beslut om teknisk spårning av en person vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om teknisk spårning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.* *En polisman som hör till befälet vid skyddspolisen beslutar om annan teknisk spårning än sådan som avses i 1 mom.* *Tillstånd får ges och beslut fattas för högst sex månader åt gången.* *I ett yrkande och i ett beslut om teknisk spårning ska följande nämnas:*

Gällande lydelse	*Föreslagen lydelse*
	1) den verksamhet som avses i 3 §, *2) den person, det föremål, det ämne eller den egendom som åtgärden riktas mot,* *3) de fakta som förutsättningarna för och inriktningen av den tekniska spårningen grundar sig på,* *4) tillståndets giltighetstid med angivande av klockslag,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar den tekniska spårningen,* *6) eventuella begränsningar och villkor för den tekniska spårningen.*
(ny)	14 § *Beslut om teknisk observation av utrustning vid civil underrättelseinhämtning* *Beslut om teknisk observation av utrustning vid civil underrättelseinhämtning ska fattas av domstol på yrkande av en polisman som hör till befälet vid skyddspolisen. Om ärendet inte tål uppskov, får en polisman som hör till befälet vid skyddspolisen besluta om teknisk observation av utrustning till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.* *Tillstånd får beviljas för högst sex månader åt gången.* *I ett yrkande och i ett beslut om teknisk observation av utrustning ska följande nämnas:* *1) den verksamhet som avses i 3 §,* *2) den tekniska anordning eller programvara som åtgärden riktas mot,* *3) de fakta som förutsättningarna för och inriktningen av den tekniska observationen av utrustning grundar sig på,* *4) tillståndets giltighetstid med angivande av klockslag,* *5) den till befälet vid skyddspolisen hörande polisman som leder och övervakar den tekniska observationen av utrustning,* *6) eventuella begränsningar och villkor för den tekniska observationen av utrustning.*

Gällande lydelse	*Föreslagen lydelse*
(ny)	15 §
	Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning vid civil underrättelseinhämtning
	Skyddspolisen får vid civil underrättelseinhämtning inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning med en teknisk anordning.
	Kommunikationsverket ska kontrollera att den tekniska anordningen inte på grund av sina egenskaper orsakar skadliga störningar i anordningar eller tjänster i allmänna kommunikationsnät.
	Beslut om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning fattas av en polisman som hör till befälet vid skyddspolisen.
(ny)	16 §
	Installation och avinstallation av anordningar, metoder eller programvara vid civil underrättelseinhämtning
	En tjänsteman som är anställd vid skyddspolisen har vid civil underrättelseinhämtning rätt att placera en anordning, metod eller programvara som används för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, optisk observation, teknisk spårning eller teknisk observation av utrustning på eller i föremål, ämnen, egendom, utrymmen, platser eller informationssystem som åtgärden riktas mot, om det behövs för användningen av metoden för underrättelseinhämtning. För att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran har en tjänsteman som är anställd vid skyddspolisen då rätt att i hemlighet ta sig in i ett ovan nämnt utrymme eller på en ovan nämnd plats eller i ett ovan nämnt informationssystem och att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemens säkerhetssystem.
	Anordningar, metoder och programvara som används för teleavlyssning, inhämtande

Gällande lydelse	*Föreslagen lydelse*
	av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, optisk observation, teknisk spårning eller teknisk observation av utrustning får installeras i utrymmen som används för stadigvarande boende endast om domstolen har gett tillstånd till det på yrkande av en polisman som hör till befälet vid skyddspolisen.
(ny)	17 §
	Framställning om och plan för en täckoperation vid civil underrättelseinhämtning
	I en framställning om en täckoperation vid civil underrättelseinhämtning ska följande nämnas: *1) den som föreslagit åtgärden,* *2) den person eller grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information,* *3) den verksamhet som avses i 3 §,* *4) de fakta som förutsättningarna för och inriktningen av täckoperationen grundar sig på,* *5) syftet med täckoperationen,* *6) behovet av täckoperationen,* *7) övriga uppgifter som behövs för att bedöma förutsättningarna för täckoperationen.* *Över en täckoperation ska en sådan skriftlig plan göras upp som innehåller väsentlig och tillräckligt detaljerad information för beslutsfattandet om och genomförandet av täckoperationen. Vid förändrade omständigheter ska planen vid behov ses över.*
(ny)	18 §
	Beslut om en täckoperation vid civil underrättelseinhämtning
	Beslut om en sådan täckoperation som avses i 17 § ska fattas av chefen för skyddspolisen. Beslut om täckoperationer som genomförs uteslutande i datanät får fattas också av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning. *Ett beslut om en täckoperation får vara i kraft högst sex månader åt gången.*

Gällande lydelse	*Föreslagen lydelse*
	Beslut om en täckoperation ska fattas skriftligen. I beslutet ska följande nämnas: *1) den som föreslagit åtgärden,* *2) den polisman som ansvarar för genomförandet av täckoperationen,* *3) identifikationsuppgifterna för de polismän som genomför täckoperationen,* *4) den verksamhet som avses i 3 §,* *5) den person eller grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information,* *6) de fakta som förutsättningarna för och inriktningen av täckoperationen grundar sig på,* *7) täckoperationens syfte och genomförandeplan,* *8) tillståndets giltighetstid,* *9) eventuella begränsningar och villkor för täckoperationen.* *Vid förändrade omständigheter ska beslutet vid behov ses över. Beslut om avslutande av en täckoperation ska fattas skriftligen.*
(ny)	19 § *Brottsförbud vid civil underrättelseinhämtning* *En polisman vid skyddspolisen som företar en täckoperation vid civil underrättelseinhämtning får inte begå brott eller ta initiativ till ett brott.* *Om en polisman vid skyddspolisen som företar en täckoperation begår en trafikförseelse, en ordningsförseelse eller något annat jämförbart brott för vilket det föreskrivna straffet är ordningsbot, går polismannen fri från straffansvar, om gärningen har varit nödvändig för att syftet med täckoperationen ska nås eller för att inhämtandet av information inte ska avslöjas.*
(ny)	20 § *Beslut om bevisprovokation genom köp vid civil underrättelseinhämtning* *Beslut om bevisprovokation genom köp vid civil underrättelseinhämtning ska fattas av chefen för skyddspolisen. Beslut om bevisprovokation genom köp som gäller säljanbud*

Gällande lydelse	*Föreslagen lydelse*
	uteslutande till allmänheten får fattas också av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning. *Beslut om bevisprovokation genom köp får meddelas för högst sex månader åt gången.* *Beslut om bevisprovokation genom köp ska fattas skriftligen. I beslutet ska följande nämnas:* *1) den verksamhet som avses i 3 §,* *2) den person som är föremål för bevisprovokation,* *3) de fakta som förutsättningarna för och inriktningen av bevisprovokationen grundar sig på,* *4) de föremål, de ämnen, den egendom eller de tjänster som är föremål för bevisprovokationen,* *5) syftet med bevisprovokationen,* *6) tillståndets giltighetstid,* *7) den till befälet vid skyddspolisen hörande polisman som leder och övervakar bevisprovokationen,* *8) eventuella begränsningar och villkor för bevisprovokationen.*
(ny)	21 § *Plan för genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning* *Över genomförandet av bevisprovokation genom köp vid civil underrättelseinhämtning ska det upprättas en skriftlig plan, om detta behövs med hänsyn till operationens omfattning eller andra motsvarande skäl.* *Vid förändrade omständigheter ska planen för genomförande av bevisprovokationen vid behov ses över.*
(ny)	22 § *Beslut om genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning* *Beslut om genomförande av bevisprovokation genom köp vid civil underrättelseinhämtning ska fattas skriftligen. Beslutet ska fattas av en för uppdraget förordnad polisman som*

Gällande lydelse	*Föreslagen lydelse*
	hör till befälet vid skyddspolisen och är förtrogen med användningen av metoder för underrättelseinhämtning och som ansvarar för genomförandet av bevisprovokationen. *I beslutet ska följande nämnas:* *1) den polisman som beslutat om bevisprovokationen genom köp samt beslutets datum och innehåll,* *2) identifikationsuppgifterna för de polismän som genomför bevisprovokationen,* *3) hur det har säkerställts att bevisprovokationen inte får den som är föremål för åtgärden eller någon annan att begå ett brott som denne annars inte skulle begå,* *4) eventuella begränsningar och villkor för bevisprovokationen.* *Om åtgärden inte tål uppskov, behöver ett beslut som avses i 2 mom. inte upprättas i skriftlig form före bevisprovokationen. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter bevisprovokationen.* *Vid förändrade omständigheter ska beslutet om genomförande av bevisprovokationen vid behov ses över.*
(ny)	23 § *Säkerheten för polismän vid förtäckt inhämtande av information, täckoperationer, bevisprovokation genom köp och användning av informationskällor vid civil underrättelseinhämtning* *En polisman som hör till befälet vid skyddspolisen får besluta att en polisman som ska genomföra sådant förtäckt inhämtande av information, en sådan täckoperation eller sådan bevisprovokation genom köp eller förbereda eller genomföra sådan användning av informationskällor som avses i detta kapitel ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att polismannens säkerhet ska kunna tryggas.* *Avlyssningen och observationen får upptas. Upptagningarna ska utplånas så snart de inte behövs för att trygga polismannens säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har samband med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i*

Gällande lydelse	*Föreslagen lydelse*
	detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller avskrivits.
(ny)	24 §
	Beslut om styrd användning av informationskällor vid civil underrättelseinhämtning
	Beslut om styrd användning av informationskällor vid civil underrättelseinhämtning fattas av chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning. *Ett beslut om styrd användning av informationskällor får vara i kraft högst sex månader åt gången.* *Beslut om styrd användning av informationskällor ska fattas skriftligen. I beslutet ska följande nämnas:* *1) den som föreslagit åtgärden,* *2) den polisman som ansvarar för genomförandet av inhämtandet av information,* *3) identifikationsuppgifterna för informationskällan,* *4) den verksamhet som avses i 3 §,* *5) de fakta som förutsättningarna för och inriktningen av den styrda användningen av in-formationskällor grundar sig på,* *6) syftet med inhämtandet av information och planen för genomförandet av detta,* *7) tillståndets giltighetstid,* *8) eventuella begränsningar och villkor för den styrda användningen av informationskällor.* *Vid förändrade omständigheter ska beslutet vid behov ses över. Beslut om avslutande av styrd användning av en informationskälla ska fattas skriftligen.* *I fråga om registrering av uppgifter om informationskällor i ett personregister och betalning av arvode tillämpas vad som föreskrivs i 5 kap. 41 §.*
(ny)	25 §
	Tryggande av informationskällor vid civil underrättelseinhämtning
	Vid civil underrättelseinhämtning kan

Gällande lydelse	*Föreslagen lydelse*
	skyddspolisen med en informationskällas samtycke övervaka informationskällans bostad, eller något annat utrymme som informationskällan använder för boende, och dess omedelbara närmiljö med kamera eller någon annan teknisk anordning, metod eller programvara som placerats på platsen, om det behövs för att avvärja en fara som hotar informationskällans liv eller hälsa. Utomstående behöver inte upplysas om att informationskällan tryggas. *Övervakningen ska avslutas utan dröjsmål, om den inte längre behövs för att avvärja en fara som hotar informationskällans liv eller hälsa.* *Upptagningar som uppkommit vid övervakning enligt 1 mom. ska utplånas så snart de inte behövs för att trygga informationskällans säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har samband med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller avskrivits.* *En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning får besluta att en informationskälla, med informationskällans samtycke, ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen i ett enskilt fall är nödvändig för att informationskällans säkerhet ska kunna tryggas. Avlyssningen och observationen får upptas. Upptagningarna ska utplånas så snart de inte behövs för att trygga informationskällans säkerhet.* *Chefen för skyddspolisen får besluta att en informationskälla ges falska, vilseledande eller förtäckta uppgifter eller registeranteckningar, som får användas i ett enskilt fall, eller att falska handlingar får upprättas för att användas av informationskällan, om det är nödvändigt för att för att skydda informationskällans liv och hälsa. En registeranteckning ska rättas när förutsättningarna enligt detta moment inte längre finns.*

Gällande lydelse	*Föreslagen lydelse*
(ny)	26 §
	Platsspecifik underrättelseinhämtning
	Med platsspecifik underrättelseinhämtning avses underrättelseinhämtning för att hitta föremål, egendom, handlingar eller information eller utröna omständigheter på någon annan plats än en plats som används för stadigvarande boende eller en plats beträffande vilken det finns anledning att anta att underrättelseinhämtningen kommer att omfatta information som någon enligt 17 kap. 11, 13, 14, 16, 20 eller 21 § eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om.
(ny)	27 §
	Beslut om platsspecifik underrättelseinhämtning vid civil underrättelseinhämtning
	Beslut om platsspecifik underrättelseinhämtning vid civil underrättelseinhämtning ska fattas av domstol, om den riktas mot någon annan hemfridsskyddad plats än ett utrymme som används för stadigvarande boende eller mot en plats som allmänheten inte har tillträde till eller dit tillträdet för allmänheten har begränsats eller förhindrats under den tid den platsspecifika underrättelseinhämtningen genomförs, på yrkande av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning. *Om det ärende som avses i 1 mom. inte tål uppskov, får chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning besluta om platsspecifik underrättelseinhämtning till dess att domstolen har avgjort yrkandet. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.* *Chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrät-*

Gällande lydelse	*Föreslagen lydelse*
	telseinhämtning beslutar om annan platsspecifik underrättelseinhämtning än sådan som avses i 1 mom. *Ett beslut om platsspecifik underrättelseinhämtning får vara i kraft högst en månad åt gången.* *I ett yrkande och i ett beslut om platsspecifik underrättelseinhämtning ska tillräckligt noggrant specificeras* *1) den verksamhet som avses i 3 §,* *2) den plats som är föremål för den platsspecifika underrättelseinhämtningen,* *3) de fakta utifrån vilka det anses finnas förutsättningar för platsspecifik underrättelseinhämtning,* *4) vad som söks, i den utsträckning det är möjligt att ange, genom den platsspecifika underrättelseinhämtningen,* *5) eventuella begränsningar i den platsspecifika underrättelseinhämtningen.* *När sakens brådskande natur kräver det får ett beslut om platsspecifik underrättelseinhämtning dokumenteras efter det att den platsspecifika underrättelseinhämtningen har genomförts.* *Om det medan en platsspecifik underrättelseinhämtning pågår framkommer att underrättelseinhämtningen har omfattat sådan information som någon enligt 17 kap. 11, 13, 14, 16, 20 eller 21 § eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om, ska underrättelseinhämtningen till denna del genast avslutas och de anteckningar och kopior som gäller informationen genast utplånas eller förstöras.*
(ny)	28 § *Kopiering vid civil underrättelseinhämtning* *Skyddspolisen har vid civil underrättelseinhämtning rätt att kopiera handlingar och föremål.*
(ny)	29 § *Kopieringsförbud vid civil underrättelseinhämtning* *En handling eller något annat objekt som avses i 26 § får inte kopieras vid civil under-*

Gällande lydelse	*Föreslagen lydelse*
	rättelseinhämtning, om objektet innehåller sådant som någon med stöd av 17 kap. 11, 13, 14, 16, 20 eller 21 § i rättegångsbalken har skyldighet eller rätt att vägra vittna om. *Om tystnadsplikten eller tystnadsrätten grundar sig på 17 kap. 11 § 2 eller 3 mom. i rättegångsbalken eller 13, 14, 16 eller 20 § i det kapitlet, är en förutsättning för förbudet utöver det som föreskrivs i 1 mom. dessutom att objektet innehas av en person som avses i bestämmelsen i fråga eller av någon som står i ett sådant förhållande till honom eller henne som avses i 17 kap. 22 § 2 mom. i rättegångsbalken, eller av den till vars förmån tystnadsplikten eller tystnadsrätten har föreskrivits.* *Kopieringsförbud gäller dock inte, om* *1) den i 17 kap. 11 § 2 eller 3 mom., 13 § 1 eller 3 mom., 14 § 1 mom. eller 16 § 1 mom. i rättegångsbalken avsedda person till vars förmån tystnadsplikten har föreskrivits samtycker till kopiering,* *2) en i 17 kap. 20 § 1 mom. i rättegångsbalken avsedd person samtycker till kopiering.*
(ny)	30 § *Kopieringsförbud som gäller teleavlyssning, teleövervakning och basstationsuppgifter* *Handlingar och data som innehas av ett i 3 § 27 punkten i lagen om tjänster inom elektronisk kommunikation avsett teleföretag (teleföretag) eller en i 36 punkten i den paragrafen avsedd sammanslutningsabonnent och som innehåller uppgifter om meddelanden som avses i 5 kap. 5 § 1 mom. i denna lag eller innehåller identifieringsuppgifter som avses i 5 kap. 8 § 1 mom. eller basstationsuppgifter som avses i 5 kap. 11 § 1 mom. får inte kopieras.*
(ny)	31 § *Kopiering av försändelser vid civil underrättelseinhämtning* *Skyddspolisen har vid civil underrättelseinhämtning rätt att kopiera ett brev eller en annan försändelse innan den anländer till*

Gällande lydelse	*Föreslagen lydelse*
	mottagaren.
(ny)	32 §
	Kvarhållande av försändelser för kopiering
	Om det finns skäl att anta att ett brev eller någon annan försändelse som får kopieras vid civil underrättelseinhämtning kommer att anlända till eller redan finns vid ett verksamhetsställe för post, en järnvägsstation eller en del av en sådan eller ett verksamhetsställe som innehas av den som yrkesmässigt transporterar försändelser i samband med trafik eller annars, får en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning förordna att försändelsen ska hållas kvar på verksamhetsstället i fråga tills kopiering hinner utföras. *Det förordnande som avses i 1 mom. får meddelas för högst en månad räknat från det att chefen för verksamhetsstället har fått kännedom om förordnandet. Försändelsen får inte utan tillåtelse av den tjänsteman som avses i 1 mom. överlämnas till någon annan än tjänstemannen eller till den som han eller hon har utsett.* *Chefen för verksamhetsstället ska genast underrätta den som meddelat föreläggandet om när försändelsen har anlänt. Denne ska utan ogrundat dröjsmål besluta om kopiering.*
(ny)	33 §
	Beslut om kopiering
	Beslut om kopiering vid civil underrättelseinhämtning ska fattas av en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning. *Om ett ärende inte tål uppskov, får också någon annan polisman vid skyddspolisen än en sådan som avses i 1 mom. i ett enskilt fall besluta om kopiering, till dess att en tjänsteman som avses i 1 mom. har avgjort ärendet. Ärendet ska lämnas över till en polisman som*

Gällande lydelse	*Föreslagen lydelse*
	avses i 1 mom. för avgörande så snart det är möjligt, dock senast 24 timmar efter det att metoden för inhämtande av information började användas.
(ny)	34 § *Förstöring av kopior* *En kopia ska förstöras utan dröjsmål, om det framgår att sådant material har kopierats som det är förbjudet att kopiera eller att informationen inte behövs för att skydda den nationella säkerheten.*
(ny)	35 § *Förfarandet i domstol i ärenden som gäller civil underrättelseinhämtning* *Ett tillståndsärende som gäller en metod för civil underrättelseinhämtning ska handläggas av Helsingfors tingsrätt. Tingsrätten är domför med ordföranden ensam. Sammanträdet kan hållas även vid en annan tidpunkt och på en annan plats än vad som förskrivs om en allmän underrätts sammanträde.* *Ett yrkande om användning av en metod för underrättelseinhämtning ska göras skriftligen. Ett yrkande som gäller användning av en metod för underrättelseinhämtning ska utan dröjsmål tas upp till behandling i domstol i närvaro av den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman som är insatt i ärendet.* *Ärendet ska avgöras skyndsamt. Behandlingen kan också ske med anlitande av videokonferens eller någon annan lämplig teknisk dataöverföring där de som deltar i behandlingen har sådan kontakt att de kan tala med och se varandra.* *I fråga om varje metod för underrättelseinhämtning finns det särskilda bestämmelser om innehållet i beslutet. Beslutet ska meddelas omedelbart eller senast när behandlingen av de ärenden om metoder för underrättelseinhämtning som anknyter till samma underrättelsehelhet har avslutats.*

Gällande lydelse	*Föreslagen lydelse*
	Om domstolen har beviljat tillstånd till teleavlyssning eller teleövervakning, får den pröva och avgöra ett ärende som gäller beviljande av tillstånd i fråga om en ny person, teleadress eller teleterminalutrustning utan att den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman är närvarande, om det har förflutit mindre än sex månader från den muntliga förhandlingen av det tidigare tillståndsärendet. Ärendet kan behandlas utan att tjänstemannen är närvarande också om användningen av metoden för underrättelseinhämtning redan har avslutats. *Ett beslut i ett tillståndsärende får inte överklagas genom besvär. Klagan mot beslutet får anföras utan tidsbegränsning hos Helsingfors hovrätt. Klagan ska behandlas skyndsamt.* *Vid handläggningen av ett ärende som gäller en metod för underrättelseinhämtning ska det fästas särskild vikt vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.*
(ny)	36 § *Skyddande av civil underrättelseinhämtning* *Skyddspolisen får använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt upprätta och använda falska handlingar, om det är nödvändigt för att skydda den civila underrättelseinhämtningen.* *En registeranteckning som avses i 1 mom. ska rättas när förutsättningarna enligt det momentet inte längre finns.*
(ny)	37 § *Beslut om skyddande* *Beslut om registeranteckningar och upprättande av handlingar enligt 36 § 1 mom. ska fattas av chefen för skyddspolisen.* *En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är*

Gällande lydelse	*Föreslagen lydelse*
	förtrogen med användningen av metoder för underrättelseinhämtning beslutar om annat än i 1 mom. avsett skyddande. *Den myndighet som har fattat beslut om registeranteckningar och upprättande av handlingar ska föra en förteckning över anteckningarna och handlingarna, övervaka användningen av dem samt se till att anteckningarna rättas.*
(ny)	38 § *Yppandeförbud vid civil underrättelseinhämtning* *En för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för civil underrättelseinhämtning får förbjuda en utomstående att röja sådana omständigheter om användningen av en metod för civil underrättelseinhämtning som denne fått kännedom om, om det är motiverat för att skydda metoden för underrättelseinhämtning. Det förutsätts dessutom att den utomstående med anledning av sitt uppdrag eller sin ställning har bistått eller blivit ombedd att bistå vid användningen av en metod för underrättelseinhämtning.* *Ett yppandeförbud meddelas för högst ett år åt gången. Förbudet ska ges i skriftlig form och bevisligen delges den som förbudet gäller. I förbudet ska det specificeras de omständigheter som förbudet omfattar, nämnas förbudets giltighetstid och anges hotet om straff för överträdelse av förbudet.* *Ett beslut om yppandeförbud får inte överklagas genom besvär. Den som har fått ett förbud får dock utan tidsbegränsning anföra klagan hos Helsingfors hovrätt. Klagan ska behandlas skyndsamt.* *Till straff för överträdelse av yppandeförbudet döms enligt 38 kap. 1 eller 2 § i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans i lag.* *Den som har fått ett yppandeförbud får trots 4 mom. meddela underrättelseombudsmannen om yppandeförbudet.*

Gällande lydelse	*Föreslagen lydelse*
(ny)	39 §
	Beslut om användning av metoder för underrättelseinhämtning i vissa fall
	Beslut om civil underrättelseinhämtning och användning av metoder för underrättelseinhämtning som sker utanför Finland ska fattas av chefen för skyddspolisen. *I fråga om innehållet i framställningar, planer, yrkanden och beslut som gäller användningen av metoder för underrättelseinhämtning tillämpas vad som i detta kapitel föreskrivs om framställningar, planer, yrkanden och beslut.* *Bestämmelserna i 4 § 4 mom., 41, 44, 46 och 47 § i detta kapitel kan tillämpas på sådan civil underrättelseinhämtning och användning av metoder för underrättelseinhämtning som avses i 1 mom.*
(ny)	40 §
	Beräkning av tidsfrister vid civil underrättelseinhämtning
	Vid beräkning av tidsfrister enligt detta kapitel ska inte lagen om beräknande av laga tid (150/1930) tillämpas. *En i månader uttryckt tid löper ut den dag i månaden som till sitt ordningsnummer motsvarar den dag då tidsfristen började löpa. Om motsvarande dag inte finns i den månad då tidsfristen löper ut, löper tiden ut den sista dagen i månaden.*
(ny)	41 §
	Förbud mot avlyssning och observation vid civil underrättelseinhämtning
	Teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation får inte riktas mot sådan kommunikation som parterna i kommunikationen inte får vittna om eller som parterna har rätt att vägra vittna om med stöd av 17 kap. 13, 14, 16, 20 § eller 22 § 2 mom. i rättegångsbalken. *Om det under tiden för teleavlyssning, inhämtande av information i stället för teleav-*

Gällande lydelse	*Föreslagen lydelse*
	lyssning, teknisk avlyssning eller optisk observation eller vid något annat tillfälle framkommer att det är fråga om ett meddelande som det är förbjudet att avlyssna eller observera, ska åtgärden avbrytas och de upptagningar som fåtts genom åtgärden och anteckningarna om de uppgifter som fåtts genom den genast utplånas. *De förbud mot avlyssning och observation som avses i denna paragraf gäller dock inte sådana fall där en i 1 mom. avsedd person deltar i sådan verksamhet som är föremål för civil underrättelseinhämtning där verksamheten allvarligt hotar den nationella säkerheten och det även för hans eller hennes del har fattats beslut om teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation.*
(ny)	42 § *Granskning av upptagningar och handlingar från civil underrättelseinhämtning* *En polisman som hör till befälet vid skyddspolisen eller en av denne förordnad tjänsteman ska utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av en metod för civil underrättelseinhämtning.*
(ny)	43 § *Undersökning av upptagningar från civil underrättelseinhämtning* *Upptagningar som uppkommit vid användningen av metoder för civil underrättelseinhämtning får undersökas endast av domstol och en polisman som hör till befälet vid skyddspolisen. Enligt förordnande av en polisman som hör till befälet vid skyddspolisen eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en expert eller av någon annan som anlitas för inhämtande av information.*

Gällande lydelse	*Föreslagen lydelse*
(ny)	44 §
	Utlämnande av information som erhållits vid civil underrättelseinhämtning för brottsbekämpning
	Skyddspolisen ska utan ogrundat dröjsmål anmäla till centralkriminalpolisen, om det medan en metod för underrättelseinhämtning används framkommer att det kan antas att ett sådant brott har begåtts för vilket det föreskrivna strängaste straffet är fängelse i minst sex år. Genom beslut av chefen för skyddspolisen får anmälan skjutas upp med högst ett år åt gången, om det är nödvändigt för att garantera den nationella säkerheten eller skydda liv eller hälsa. Skyddspolisen får anmäla ett begånget brott till centralkriminalpolisen, om det föreskrivna strängaste straffet för brottet är fängelse i minst tre år.
	Skyddspolisen ska utan dröjsmål anmäla till en behörig myndighet, om det medan en metod för underrättelseinhämtning används framkommer att ett sådant brott är på färde för vilket det föreskrivna strängaste straffet är fängelse i minst sex år och brottet ännu kan förhindras. Information som fåtts genom användning av en metod för underrättelseinhämtning får lämnas ut till en behörig myndighet för förhindrande av ett sådant brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år.
	När det övervägs om en anmälan ska skjutas upp enligt 1 mom. eller en anmälan göras enligt 1 eller 2 mom. i fråga om ett begånget brott för vilket det föreskrivna strängaste straffet är fängelse i minst tre år eller i fråga om förhindrade av ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år, ska betydelsen av utredningen eller förhindrandet av brottet med tanke på allmänna och enskilda intressen beaktas vid bedömningen.
	Information som fåtts genom användning av en metod för underrättelseinhämtning får alltid lämnas ut som utredning som stöder det att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada.
	Om en förundersökningsmyndighet inleder

Gällande lydelse	*Föreslagen lydelse*
	en förundersökning eller börjar vidta en förundersökningsåtgärd eller en behörig myndighet inleder en åtgärd som syftar till att förhindra ett brott utifrån en anmälan som avses i denna paragraf, ska förundersökningsmyndigheten eller den behöriga myndigheten innan förundersökningen inleds, förundersökningsåtgärden vidtas eller den brottsförhindrande åtgärden vidtas anmäla detta till skyddspolisen.
(ny)	45 §
	Utplåning av information som erhållits vid en metod för underrättelseinhämtning
	Information som fåtts genom en metod för underrättelseinhämtning ska utplånas utan dröjsmål efter att det framgått att den inte behövs för att skydda den nationella säkerheten. *Informationen får dock bevaras och lagras i ett register som avses i lagen om behandling av personuppgifter i polisens verksamhet, om detta behövs i fall som avses i 44 §.* *Basstationsuppgifter som avses i 7 § ska utplånas efter att det har framgått att de inte behövs för att skydda den nationella säkerheten.*
(ny)	46 §
	Utplåning av information som fåtts i en brådskande situation
	Om en polisman som hör till befälet vid skyddspolisen i en brådskande situation enligt 7 § 1 mom., 8 § 1 mom., 11 § 1 mom., 12 § 1 mom., 13 § 1 mom., 14 § 1 mom. eller 27 § 2 mom. har beslutat att teleövervakning, inhämtande av basstationsuppgifter, teknisk avlyssning, optisk observation, teknisk spårning av en person, teknisk observation av utrustning eller platsspecifik underrättelseinhämtning ska inledas, men domstolen anser att det inte har funnits förutsättningar för åtgärden, ska användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Information som fåtts

Gällande lydelse	*Föreslagen lydelse*
	på detta sätt får dock användas under samma förutsättningar som en uppgift får användas i de fall som avses i 44 § 1 eller 2 mom., om det kan antas att det har begåtts ett sådant brott för vilket det strängaste föreskrivna straffet är fängelse i minst sex år eller om det framgår att ett sådant brott är på färde för vilket det strängaste föreskrivna straffet är fängelse i minst sex år och brottet ännu kan förhindras. *Om en polisman vid skyddspolisen i en brådskande situation enligt 33 § 2 mom. har beslutat om kopiering, men en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning anser att det inte har funnits förutsättningar för åtgärden, ska användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas. Information som fåtts på detta sätt får dock användas under samma förutsättningar som en uppgift får användas i de fall som avses i 44 § 1 eller 2 mom., om det kan antas att det har begåtts ett sådant brott för vilket det strängaste föreskrivna straffet är fängelse i minst sex år eller om det framgår att ett sådant brott är på färde för vilket det strängaste föreskrivna straffet är fängelse i minst sex år och brottet ännu kan förhindras.*
(ny)	47 § *Underrättelse om användning av metod för underrättelseinhämtning* *Den person som vid civil underrättelseinhämtning har varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning och teknisk observation samt kopiering som riktar sig mot ett meddelande eller sådan kopiering av en försändelse som riktar sig mot ett meddelande ska utan dröjsmål underrättas om detta skriftligen efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts. Den som varit föremål för inhämtande av information ska dock underrättas om användningen av metoden för*

Gällande lydelse *Föreslagen lydelse*

underrättelseinhämtning senast ett år från det att användningen av metoden upphörde.

På yrkande av en polisman som hör till befälet vid skyddspolisen får domstolen besluta att underrättelsen enligt 1 mom. till den som varit föremål för åtgärden får skjutas upp med högst två år åt gången, om det är motiverat för att trygga pågående användning av en metod för underrättelseinhämtning, garantera den nationella säkerheten eller skydda liv eller hälsa. Domstolen får besluta att underrättelsen ska utebli, om det är nödvändigt för att garantera den nationella säkerheten eller skydda liv eller hälsa.

Om den som varit föremål för inhämtandet av information inte är identifierad vid utgången av den tid eller det uppskov som avses i 1 eller 2 mom., ska han eller hon utan ogrundat dröjsmål skriftligen underrättas om underrättelseinhämtningen när identiteten har utretts.

Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om underrättelsen.

Om skyddspolisen fortsätter inhämtandet av information med stöd av 5 §, ska bestämmelserna om underrättelse om hemligt inhämtande av information i 5 kap. 58 § iakttas.

Den som vid civil underrättelseinhämtning varit föremål för inhämtande av information behöver inte underrättas om systematisk observation, förtäckt inhämtande av information, en täckoperation, bevisprovokation genom köp, styrd användning av informationskällor, platsspecifik underrättelseinhämtning, kopiering som riktar sig mot annat än ett meddelande och sådan kopiering av en försändelse som riktar sig mot annat än ett meddelande, om inte förundersökning har inletts i ärendet utifrån en anmälan enligt 44 §. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen iakttas.

Den som varit föremål för inhämtande av information behöver inte underrättas om användningen av en metod för underrättelseinhämtning, om föremålet har varit en statlig aktör eller en aktör som är jämställbar med en sådan.

I fråga om handläggning av underrättelse-

Gällande lydelse	*Föreslagen lydelse*
	ärenden i domstol ska 35 § iakttas.
(ny)	48 §
	Protokoll
	Efter det att användningen av en metod för underrättelseinhämtning upphört ska det utan ogrundat dröjsmål upprättas ett protokoll över användningen av metoden.
(ny)	49 §
	Begränsning av partsoffentlighet i vissa fall
	En person vars rättigheter eller skyldigheter saken gäller har inte, trots 11 § i lagen om offentlighet i myndigheternas verksamhet (621/1999), rätt att få vetskap om användningen av en sådan metod för underrättelseinhämtning som avses i detta kapitel förrän en underrättelse enligt 47 § har gjorts. *Bestämmelser om rätt till insyn för registrerade finns i lagen om behandling av personuppgifter i polisens verksamhet.*
(ny)	50 §
	Rätt att få information av privata sammanslutningar
	Trots att en sammanslutnings medlemmar, revisorer, verkställande direktör, styrelsemedlemmar eller arbetstagare är bundna av företags-, bank- eller försäkringshemlighet har skyddspolisen på begäran av en polisman som hör till befälet vid skyddspolisen rätt att få uppgifter som i ett enskilt fall kan antas vara behövliga vid utredningen av sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten och som kan antas vara av betydelse för att *1) identifiera eller nå en fysisk eller juridisk person som är föremål för civil underrättelseinhämtning, eller klarlägga personens kontaktuppgifter eller hur personen förflyttar sig,* *2) inrikta användningen av en metod för underrättelseinhämtning på en viss person som är föremål för civil underrättelsein-*

Gällande lydelse	*Föreslagen lydelse*
	hämtning, eller *3) klarlägga ekonomisk verksamhet som antas anknyta till i 3 § avsedd verksamhet som bedrivs av en person eller en juridisk person som är föremål för civil underrättelseinhämtning.*
(ny)	51 § *Teleföretags skyldighet att biträda civil underrättelseinhämtning* *På teleföretags skyldighet att biträda vid civil underrättelseinhämtning tillämpas vad som i 5 kap. 61 § föreskrivs om teleföretags skyldighet att biträda.*
(ny)	52 § *Ersättningar till teleföretag för biträde och lämnande av uppgifter vid civil underrättelseinhämtning* *På teleföretags rätt till ersättning för direkta kostnader som orsakats av att de biträtt myndigheter och lämnat uppgifter vid civil underrättelseinhämtning tillämpas bestämmelserna i 5 kap. 62 §.*
(ny)	53 § *Användning av uppgifter som lagras av teleföretag och hänför sig till civil underrättelseinhämtning* *Utöver vad som i 157 § 1 mom. i lagen om tjänster inom elektronisk kommunikation föreskrivs om användning av lagrade uppgifter får lagrade uppgifter som hänför sig till civil underrättelseinhämtning också användas om uppgifterna med fog kan antas vara av synnerlig vikt för att få information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten.*

Gällande lydelse	*Föreslagen lydelse*
(ny)	54 §
	Samarbete med militärunderrättelsemyndigheterna
	Skyddspolisen ska samarbeta med militärunderrättelsemyndigheterna för att den civila och militära underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt och i detta syfte, trots det som föreskrivs om sekretess, ge militärunderrättelsemyndigheterna behövliga uppgifter.
(ny)	55 §
	Samarbete med andra myndigheter och sammanslutningar
	Skyddspolisen ska enligt behov agera i samarbete med andra myndigheter för att den civila underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt. *Skyddspolisen får för att genomföra sitt uppdrag avseende civil underrättelseinhämtning agera i samarbete med sammanslutningar samt till andra myndigheter och sammanslutningar trots sekretessbestämmelserna lämna ut uppgifter, om utlämnandet av uppgifterna är nödvändigt för att skydda den nationella säkerheten.* *Bestämmelser om utlämnande av information för brottsbekämpning finns i 44 §.*
(ny)	56 §
	Samordning av hemlig informationsinhämtning
	Användningen av de metoder för underrättelseinhämtning om vilka det föreskrivs i detta kapitel ska vid behov samordnas för att säkerställa arbetssäkerheten för skyddspolisens, militärunderrättelsemyndigheternas, centralkriminalpolisens och andra myndigheters tjänstemän samt för att förhindra att de taktiska och tekniska metoder och planer som nämnda myndigheter använder vid hemlig informationsinhämtning avslöjas.

Gällande lydelse	*Föreslagen lydelse*
(ny)	57 §
	Internationellt samarbete
	Skyddspolisen får samarbeta och inhämta information tillsammans med utländska säkerhets- och underrättelsetjänster för att skydda den nationella säkerheten.
	Om gemensam informationsinhämtning genomförs i samarbete med den stat, på vars territorium metoder för underrättelseinhämtning är avsedda att användas, ska en polisman vid skyddspolisen iaktta de begränsningar och villkor för användningen av metoderna för underrättelseinhämtning som staten i fråga ställer.
	Chefen för skyddspolisen beslutar om deltagande i internationellt samarbete och om användning av metoder för underrättelseinhämtning i samband med det. En främmande stats behöriga tjänsteman har genom beslut av chefen för skyddspolisen rätt att på finskt territorium för att skydda den nationella säkerheten agera i samarbete med skyddspolisen, och under uppsikt och övervakning av en polisman vid skyddspolisen använda sådana metoder för underrättelseinhämtning om vars användning beslut fattas i enlighet med 9, 10, 18, 20 och 24 §.
	Skyddspolisen får vid internationellt samarbete, trots sekretessbestämmelserna, lämna ut information, om utlämnandet av informationen behövs för att skydda den nationella säkerheten och utlämnandet inte strider mot ett nationellt intresse.
	Bestämmelser om utlämnande av personuppgifter finns i lagen om behandling av personuppgifter i polisens verksamhet.
(ny)	58 §
	Samordning av underrättelseverksamheten
	Den civila och den militära underrättelseverksamheten samordnas mellan republikens president, statsrådets kansli, utrikesministeriet, försvarsministeriet och inrikesministeriet samt vid behov andra ministerier och myndigheter.
	Om det bedöms att den civila underrättelseverksamheten har utrikes- och säkerhets-

Gällande lydelse	*Föreslagen lydelse*
	politiska konsekvenser, ska ärendet förberedelsevis behandlas mellan de myndigheter som avses i 1 mom.
(ny)	59 §
	Inrikesförvaltningens övervakning av den civila underrättelseinhämtningen
	Det inhämtande av information som avses i detta kapitel övervakas av chefen för skyddspolisen och av inrikesministeriet.
(ny)	60 §
	Extern övervakning av den civila underrättelseinhämtningen
	Inrikesministeriet ska årligen till riksdagens justitieombudsman och underrättelseombudsmannen lämna en berättelse om hur de i detta kapitel avsedda metoderna för underrättelseinhämtning har använts och användningen övervakats samt hur det i detta kapitel avsedda skyddandet av den civila underrättelseinhämtningen har använts och användningen övervakats. *Bestämmelser om den övervakning som underrättelseombudsmannen utövar finns i lagen om övervakning av underrättelseverksamheten (/).*
(ny)	61 §
	Anmälningar till underrättelseombudsmannen
	Skyddspolisen ska informera underrättelseombudsmannen om de tillstånd och beslut som gäller användning av en metod för underrättelseinhämtning och som har meddelats med stöd av detta kapitel så snart som möjligt efter det att tillståndet beviljades eller beslutet fattades. *Skyddspolisen ska så snart som möjligt informera underrättelseombudsmannen om ett beslut som gäller* *1) skyddande av civil underrättelseverksamhet,* *2) yppandeförbud,*

Gällande lydelse	*Föreslagen lydelse*
	3) uppskjutande av en anmälan enligt 44 § 1 mom. *Vid underrättelse om ett beslut som gäller en metod för underrättelseinhämtning ska det fästas särskild vikt vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.*
(ny)	62 § *Bemyndigande att utfärda förordning* Genom förordning av statsrådet får det *utfärdas bestämmelser om* *1) hur användningen av metoder för underrättelseinhämtning och skyddandet av dem ska ordnas,* *2) dokumenteringen av åtgärderna för övervakningen,* *3) de redogörelser som ska lämnas för övervakningen av den civila underrättelseinhämtningen,* *4) förfarandet vid överföring av uppgifter som ska lämnas ut för brottsbekämpning,* *5) hur samarbetet mellan skyddspolisen och militärunderrättelsemyndigheterna ska ordnas,* *6) hur samarbetet mellan skyddspolisen och andra myndigheter ska ordnas,* *7) hur samordningen av den hemliga informationsinhämtningen* ska ordnas, 8) hur samordningen av *underrättelseverksamheten ska ordnas.* *Genom förordning av inrikesministeriet får det utfärdas bestämmelser om* *1) hur övervakningen av den civila underrättelseverksamheten ska ordnas inom inrikesförvaltningen,* *2) hur samarbetet mellan skyddspolisen och den övriga inrikesförvaltningen ska ordnas,* *3) hur skyddspolisens internationella samarbete ska ordnas.*

Gällande lydelse	*Föreslagen lydelse*
9 kap.	9 kap.
Särskilda bestämmelser	**Särskilda bestämmelser**
10 §	10 §
Närmare bestämmelser	*Närmare bestämmelser*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Genom förordning av inrikesministeriet kan närmare bestämmelser utfärdas om 1) hur polismäns ställning ska anges och polismän identifieras, 2) förvaring av egendom som tagits om hand, 3) polisundersökning, 4) tecken och metoder vid stoppande av fordon, 5) automatisk övervakning av vägtrafiken, 6) definitioner av användningen av maktmedel, utbildning i användningen av maktmedel, träning i och uppföljning av användningen av maktmedel, rätt att bära maktmedelsredskap, förvaring av maktmedelsredskap och övervakning av användningen av maktmedel, 7) fasttagande, förvaring och avlivande av djur, 8) handräckning till andra än tullverket och gränsbevakningsväsendet, 9) registrering av polisåtgärder, 10) tekniskt utförande av säkerhetskontrollåtgärder, hur säkerhetskontroller ska ordnas i praktiken och om ordnande av säkerhetskontrollutbildning, 11) uniformsmodeller och märken som ska användas med uniform samt om när tjänsteuppgifterna är av sådan art eller karaktär att de förutsätter användning av uniform.	Genom förordning av inrikesministeriet kan närmare bestämmelser utfärdas om 1) hur polismäns ställning ska anges och polismän identifieras, 2) förvaring av egendom som tagits om hand, 3) polisundersökning, 4) tecken och metoder vid stoppande av fordon, 5) automatisk övervakning av vägtrafiken, 6) definitioner av användningen av maktmedel, utbildning i användningen av maktmedel, träning i och uppföljning av användningen av maktmedel, rätt att bära maktmedelsredskap, förvaring av maktmedelsredskap och övervakning av användningen av maktmedel, 7) fasttagande, förvaring och avlivande av djur, 8) handräckning till andra än *Tullen* och *G*ränsbevakningsväsendet, 9) registrering av polisåtgärder, 10) tekniskt utförande av säkerhetskontrollåtgärder, hur säkerhetskontroller ska ordnas i praktiken och om ordnande av säkerhetskontrollutbildning, 11) uniformsmodeller och märken som ska användas med uniform samt om när tjänsteuppgifterna är av sådan art eller karaktär att de förutsätter användning av uniform. ——— *Denna lag träder i kraft den 20 .* ———

3.

Lag

om ändring av 10 och 15 a § i polisförvaltningslagen

I enlighet med riksdagens beslut
ändras i polisförvaltningslagen (110/1992) 10 § 1 och 2 mom.,
sådana de lyder i lag 860/2015, och
fogas till 15 a §, sådan den lyder i lagarna 873/2011, 1165/2013 och 421/2017, ett nytt 3 mom., i stället för det 3 mom. som upphävts genom lag 1165/2013, som följer:

Gällande lydelse	*Föreslagen lydelse*
10 §	10 §
Skyddspolisen	*Skyddspolisen*
Skyddspolisen har till uppgift att i enlighet med inrikesministeriets styrning bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet samt att utföra undersökning av sådana brott. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att förebygga verksamhet som äventyrar rikets säkerhet.	Skyddspolisen har till uppgift att i enlighet med inrikesministeriets styrning *inhämta information för att skydda den nationella säkerheten samt upptäcka, förhindra och avslöja sådan verksamhet, sådana förehavanden och* sådana brott *som kan hota statsskicket och samhällsordningen* eller rikets inre eller yttre säkerhet. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att *upptäcka och förhindra* verksamhet som *hotar samhällets* säkerhet.
Inrikesministeriet bestämmer efter att ha hört Polisstyrelsen *närmare vilka kategorier av ärenden som ska undersökas av skyddspolisen och bestämmer efter att ha hört Polisstyrelsen* vid behov närmare om samverkan och samarbetet mellan skyddspolisen och övriga polisenheter *och om undersökningsarrangemangen i förhållandet mellan dem.*	Inrikesministeriet bestämmer, efter att ha hört Polisstyrelsen, *vid behov* närmare om samverkan och samarbetet mellan skyddspolisen och andra polisenheter.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(ny)	15 a §
	Polisbefogenheter
	— — — — — — — — — — — — — — —
	Utöver det som föreskrivs i 1 mom. har en tjänsteman vid skyddspolisen rätt att använda i 5 a kap. i polislagen avsedda metoder för underrättelseinhämtning för att skydda den nationella säkerheten i enlighet med vad som föreskrivs i det kapitlet.
	_____
	Denna lag träder i kraft den 20 .
	_____

4.

Lag

om ändring av lagen om behandling av personuppgifter i polisens verksamhet

I enlighet med riksdagens beslut

ändras i lagen om behandling av personuppgifter i polisens verksamhet (761/2003) 5 § 2 mom., 13 § 1 mom. 2, 4, 6, 15 och 16 punkten och 45 § 1 mom. 5 punkten,

av dem 13 § 1 mom. 2 punkten sådan den lyder i lag 1073/2015, 13 § 4 och 6 punkten sådana de lyder i lag 457/2009 och 13 § 15 och 16 punkten sådana de lyder i lag 29/2015 samt 45 § 1 mom. 5 punkten sådan den lyder i lag 1181/2013, som följer:

Gällande lydelse	*Föreslagen lydelse*
5 §	5 §
Skyddspolisens funktionella informationssystem	*Skyddspolisens funktionella informationssystem*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Skyddspolisens funktionella informationssystem kan innehålla uppgifter som skyddspolisen måste behandla för att kunna förebygga och utreda förehavanden eller brott som äventyrar rätts- och samhällsordningen eller statens säkerhet.	Skyddspolisens funktionella informationssystem kan innehålla uppgifter som skyddspolisen måste behandla för att kunna *skydda den nationella säkerheten eller för att kunna förhindra, avslöja eller* utreda förehavanden eller brott som äventyrar rätts- och samhällsordningen eller statens säkerhet.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
13 §	13 §
Polisens rätt att få uppgifter ur vissa register och informationssystem	*Polisens rätt att få uppgifter ur vissa register och informationssystem*
Utöver vad som föreskrivs i någon annan lag har polisen trots sekretessbestämmelserna rätt att i enlighet med vad som avtalas om saken med den registeransvarige i fråga ur vissa register genom en teknisk anslutning eller som en datamängd få sådan information som polisen behöver för att utföra sina uppdrag och föra sina personregister, enligt följande:	Utöver vad som föreskrivs i någon annan lag har polisen trots sekretessbestämmelserna rätt att i enlighet med vad som avtalas om saken med den registeransvarige i fråga ur vissa register genom en teknisk anslutning eller som en datamängd få sådan information som polisen behöver för att utföra sina uppdrag och föra sina personregister, enligt följande:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
2) uppgifter som gäller dömda, fångar eller intagna i en enhet vid Brottspåföljdsmyndigheten ur Brottspåföljdsmyndighetens informationssystem som avses i 14 § 1 och 2 mom. i lagen om behandling av personuppgifter vid Brottspåföljdmyndigheten (1069/2015) för	2) uppgifter som gäller dömda, fångar eller intagna i en enhet vid Brottspåföljdsmyndigheten ur Brottspåföljdsmyndighetens informationssystem som avses i 14 § 1 och 2 mom. i lagen om behandling av personuppgifter vid Brottspåföljdmyndigheten (1069/2015) *för*

Gällande lydelse	*Föreslagen lydelse*
förhindrande, utredning och överlämnande för åtalsprövning av brott eller för ett sådant tillstånd eller godkännande från polisen som förutsätter att personen i fråga är tillförlitlig,	*skyddande av den nationella säkerheten*, för förhindrande, *avslöjande,* utredning *av brott* och överlämnande av brott *till* åtalsprövning *och* för ett sådant tillstånd eller godkännande från polisen som förutsätter att personen i fråga är tillförlitlig,
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
4) av dem som utövar inkvarteringsverksamhet sådana uppgifter om resande som avses i 6 § 1 mom. i lagen om inkvarterings- och förplägnadsverksamhet (308/2006) och som behövs för att upprätthålla allmän ordning och säkerhet samt för att förhindra, avslöja eller utreda brott och för att utföra något annat för polisen lagstadgat uppdrag,	4) av dem som utövar inkvarteringsverksamhet sådana uppgifter om resande som avses i 6 § 1 mom. i lagen om inkvarterings- och förplägnadsverksamhet (308/2006) och som behövs för *att skydda den nationella säkerheten*, upprätthålla allmän ordning och säkerhet samt för att förhindra, avslöja eller utreda brott och för att utföra något annat för polisen lagstadgat uppdrag,
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
6) ur Patent- och registerstyrelsens handelsregister, för förhindrande, avslöjande och utredande av brott, uppgifter om anmälningar och meddelanden som gäller näringsidkare,	6) ur Patent- och registerstyrelsens handelsregister, *för skyddande av den nationella säkerheten och* för förhindrande, avslöjande och utredande av brott, uppgifter om anmälningar och meddelanden som gäller näringsidkare,
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
15) ur det register över laddare som avses i 3 § i lagen om laddare (219/2000) uppgifter för övervaknings- och larmuppdrag samt för förhindrande, utredning och avslöjande av brott,	15) ur det register över laddare som avses i 3 § i lagen om laddare (219/2000) uppgifter för övervaknings- och larmuppdrag samt för *skyddande av den nationella säkerheten och* för förhindrande, utredning och avslöjande av brott,
16) av samfund och sammanslutningar uppgifter ur register som gäller passagerare och fordons personal, för förhindrande, avslöjande och utredning av brott, för överlämnande till åtalsprövning samt för att nå efterlysta personer.	16) av samfund och sammanslutningar uppgifter ur register som gäller passagerare och fordons personal, *för skyddande av den nationella säkerheten,* för förhindrande, avslöjande och utredning av brott och överlämnande av brott till åtalsprövning samt för att nå efterlysta personer.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
45 §	45 §
Inskränkningar i rätten till insyn	*Inskränkningar i rätten till insyn*
Rätten till insyn gäller inte	Rätten till insyn gäller inte
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
5) uppgifter som fåtts genom de inhämtningsmetoder som avses i 5 kap. i polislagen, 10 kap. i tvångsmedelslagen samt 36 § i lagen om dataskydd vid elektronisk kommunikation,	5) uppgifter som *erhållits vid utövande av befogenheterna enligt 4 kap. 3 § eller 5 eller 5 a kap. i polislagen, befogenheterna enligt 10 kap. i tvångsmedelslagen eller befogenheterna enligt lagen om civil underrättelseinhämtning avseende datatrafik (/),*

Gällande lydelse	*Föreslagen lydelse*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

5.

Lag

om ändring av 2 kap. 1 § i förundersökningslagen

I enlighet med riksdagens beslut
ändras i förundersökningslagen (805/2011) 2 kap. 1 § 1 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
2 kap	2 kap.
Vilka som deltar i förundersökning	**Vilka som deltar i förundersökning**
1 §	1 §
Myndigheterna vid förundersökning	*Myndigheterna vid förundersökning*
Förundersökning görs av polisen.	Förundersökning görs av *någon annan* polis *än skyddspolisen*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

7.

Lag

om ändring av 2 och 10 kap. i tvångsmedelslagen

I enlighet med riksdagens beslut

ändras i tvångsmedelslagen (806/2011) 2 kap. 9 § samt 10 kap. 3 § 1 mom., 6 § 1 mom. och 39 § 1 mom., av dem 2 kap. 9 § sådan den lyder delvis ändrad i lag 1146/2013, som följer:

Gällande lydelse	*Föreslagen lydelse*
2 kap	2 kap.
Gripande, anhållande och häktning	**Gripande, anhållande och häktning**
9 §	9 §
Anhållningsberättigade tjänstemän	*Anhållningsberättigade tjänstemän*
En anhållningsberättigad tjänsteman beslutar om anhållande. Anhållningsberättigade tjänstemän är	En anhållningsberättigad tjänsteman beslutar om anhållande. Anhållningsberättigade tjänstemän är
1) polisöverdirektören, vid Polisstyrelsen polisdirektör, polisöverinspektör och polisinspektör, polischef, biträdande polischef, vid centralkriminalpolisen chefen för centralkriminalpolisen och biträdande chef, *vid skyddspolisen chefen för skyddspolisen, biträdande chef som förordnats att sköta förundersökningsuppgifter, avdelningschef som förordnats att sköta förundersökningsuppgifter, överinspektör och inspektör som förordnats att sköta förundersökningsuppgifter,* kriminalöverinspektör, kriminalinspektör, kriminalöverkommissarie, överkommissarie, kriminalkommissarie och kommissarie,	1) polisöverdirektören, vid Polisstyrelsen polisdirektör*er*, polisöverinspektör*er* och polisinspektör*er*, polischef*er*, biträdande polischef*er*, vid centralkriminalpolisen chefen för centralkriminalpolisen och biträdande chef*er*, kriminalöverinspektörer, kriminalinspektörer, kriminalöverkommissarier, överkommissarier, kriminalkommissarier och kommissarier,
2) Tullens brottsbekämpningschef, chefen för verksamhetsenheten för Tullens brottsbekämpning och de tullöverinspektörer som av Tullens brottsbekämpningschef har förordnats till undersökningsledare,	2) Tullens brottsbekämpningschef, chefen för verksamhetsenheten för Tullens brottsbekämpning och de tullöverinspektörer *vid Tullens brottsbekämpning* som av Tullens brottsbekämpningschef har förordnats till undersökningsledare,
3) chefen och biträdande chefen för gränsbevakningsväsendet, avdelningschefen för gräns- och sjöavdelningen vid staben för gränsbevakningsväsendet, avdelningschefen, biträdande avdelningschefen, enhetschefen vid enheten för brottsbekämpning, överinspektörerna för gränsbevakningsfrågor, överinspektörerna, kriminalöverinspektörerna och kriminalinspektörerna på juridiska avdelningen vid staben för gränsbevakningsväsendet, kommendörerna och biträdande kom-	3) chefen och biträdande chefen för *G*ränsbevakningsväsendet, avdelningschefen för gräns- och sjöavdelningen vid staben för *G*ränsbevakningsväsendet, avdelningschefen, biträdande avdelningschefen, enhetschefen vid enheten för brottsbekämpning, överinspektörerna för gränsbevakningsfrågor, överinspektörerna, kriminalöverinspektörerna och kriminalinspektörerna på juridiska avdelningen vid staben för *G*ränsbevakningsväsendet, kommendörerna och biträdande

Gällande lydelse	*Föreslagen lydelse*
mendörerna för gränsbevaknings- och sjöbevakningssektionerna, chefen för en gränsbyrå eller sjöbyrå vid en gränsbevaknings- eller sjöbevakningssektion, chefen och biträdande chefen för Helsingfors gränskontrollavdelning vid Finska vikens sjöbevakningssektion och en sådan gränsbevakningsman med minst löjtnants grad som genomgått den utbildning som föreskrivs för undersökningsledare inom gränsbevakningsväsendet och som av chefen för gränsbevakningsväsendet eller chefen för någon av dess förvaltningsenheter har förordnats till undersökningsledare,	kommendörerna för gränsbevaknings- och sjöbevakningssektionerna, chefen för en gränsbyrå eller sjöbyrå vid en gränsbevaknings- eller sjöbevakningssektion, chefen och biträdande chefen för Helsingfors gränskontrollavdelning vid Finska vikens sjöbevakningssektion och en sådan gränsbevakningsman med minst löjtnants grad som genomgått den utbildning som föreskrivs för undersökningsledare inom *G*ränsbevakningsväsendet och som av chefen för *G*ränsbevakningsväsendet eller chefen för någon av dess förvaltningsenheter har förordnats till undersökningsledare,
4) åklagaren.	4) åklagare.
I fråga om anhållningsberättigade tjänstemän vid försvarsmakten föreskrivs särskilt *i lag*.	I fråga om anhållningsberättigade tjänstemän vid försvarsmakten föreskrivs särskilt.
10 kap	10 kap.
Hemliga tvångsmedel	**Hemliga tvångsmedel**
3 §	3 §
Teleavlyssning och dess förutsättningar	*Teleavlyssning och dess förutsättningar*
Med t*eleavlyssning* avses att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett sådant allmänt kommunikationsnät eller ett sådant därtill anslutet kommunikationsnät som avses i kommunikationsmarknadslagen avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 6 §. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en person som är misstänkt för brott.	Med *teleavlyssning* avses att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom *ett i 3 § 43 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) avsett allmänt kommunikationsnät eller ett* därtill anslutet kommunikationsnät avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i 6 §. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en person som är misstänkt för brott.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
6 §	6 §
Teleövervakning och dess förutsättningar	*Teleövervakning och dess förutsättningar*
Med *teleövervakning* avses att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kom-	Med *teleövervakning* avses att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kom-

Gällande lydelse	*Föreslagen lydelse*
munikationsnät som avses i 3 § eller som har mottagits till en sådan adress eller *sådan* utrustning och att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att det tillfälligt förhindras att adressen eller utrustningen används. Med *identifieringsuppgifter* avses i 2 § 8 punkten i lagen om dataskydd vid elektronisk kommunikation avsedda uppgifter om ett meddelande vilka kan förknippas med en abonnent eller användare och behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.	munikationsnät som avses i 3 § eller som har mottagits till en sådan adress eller utrustning *samt* att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att *användningen av* adressen eller utrustningen tillfälligt förhindras. Med *identifieringsuppgifter* avses *sådana uppgifter om ett meddelande som kan förknippas med en i 3 § 7* punkten i lagen om *tjänster inom* elektronisk kommunikation avsed*d användare eller med en i 30 punkten i den paragrafen avsedd abonnent och som* behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.
39 §	39 §
Användning av informationskällor och förutsättningar för styrd användning av informationskällor	*Användning av informationskällor och förutsättningar för styrd användning av informationskällor*
Med *användning av informationskällor* avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för utredning av ett brott av personer som inte hör till polisen eller till någon annan *förundersöknings*myndighet *(informationskälla)*.	Med *användning av informationskällor* avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för *skötseln av i 1 kap. 1 § avsedda uppgifter* av personer som inte hör till polisen eller till någon annan myndighet (*informationskälla*).

Denna lag träder i kraft den 20 .

8.

Lag

om ändring av lagen om offentlighet vid rättegång i allmänna domstolar

I enlighet med riksdagens beslut

ändras i lagen om offentlighet vid rättegång i allmänna domstolar (370/2007) 5 § 1 och 2 mom., 12 § 2 mom. och 16 § 4 mom.,

sådana de lyder, 5 § 2 mom. och 16 § 4 mom. i lag 1159/2013 och 12 § 2 mom. i lagarna 821/2011, 633/2015 och 13/2016, och

fogas till 5 § ett nytt 3 mom., till 12 § 2 mom. en ny 3 a-punkt och till 16 § ett nytt 5 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
5 §	5 §
Tidpunkten för när de grundläggande uppgifterna om en rättegång blir offentliga	*Tidpunkten för när de grundläggande uppgifterna om en rättegång blir offentliga*
De grundläggande uppgifter om rättegången som avses i 4 § blir genast offentliga, om inte något annat följer av 2 mom.	De grundläggande uppgifter om rättegången som avses i 4 § blir genast offentliga, om inte något annat följer av 2 och *3 mom*.
I ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen (806/2011) *eller enligt* 5 kap. i polislagen (872/2011) eller tullåtgärder enligt 20 f § i tullagen (1466/1994) och i vilket den som är föremål för metoden för inhämtande av information eller åtgärder inte behöver höras vid behandlingen av yrkandet på metoden eller åtgärder, blir de grundläggande uppgifterna offentliga först när den som misstänks för brott eller är föremål för metoden eller åtgärder senast ska underrättas om att sådana använts. Om personen i fråga underrättas om användningen av metoden eller åtgärderna senare därför att hans eller hennes identitet inte har varit känd, blir de grundläggande uppgifterna offentliga när domstolen informeras om underrättelsen. Domstolen får besluta att de grundläggande uppgifterna ska bli offentliga tidigare.	I ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen (806/2011), 5 kap. i polislagen (872/2011) *eller 3 kap. i lagen om brottsbekämpning inom Tullen (623/2015) eller som gäller en metod för underrättelseinhämtning enligt 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik (/) eller lagen om militär underrättelseverksamhet (/)* och i vilket den som är föremål för metoden *inte behöver höras vid behandlingen av yrkandet på metoden,* blir de grundläggande uppgifterna offentliga först när den som misstänks för brott eller är föremål för metoden senast ska underrättas om att sådana metoder använts. Om personen i fråga underrättas om användningen av metoden senare därför att hans eller hennes identitet inte har varit känd, blir de grundläggande uppgifterna offentliga när domstolen informeras om underrättelsen. Domstolen får besluta att de grundläggande uppgifterna ska bli offentliga tidigare. *I ett ärende som gäller ett i 15 § i lagen om övervakning av underrättelseverksamheten (/) avsett interimistiskt förordnande av underrättelseombudsmannen tillämpas i fråga om tidpunkten för när uppgifterna blir offentliga bestämmelserna i 2 mom.*

Gällande lydelse	*Föreslagen lydelse*
12 §	12 §
En parts rätt att ta del av en handling	*En parts rätt att ta del av en handling*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
En parts rätt enligt 1 mom. gäller inte 1) information som avses i 11 § 2 mom. 7 och 7 a-punkten i lagen om offentlighet i myndigheternas verksamhet, 2) rättegångshandlingar som upprättats vid en domstol, före den tidpunkt som avses i 8 §, 3) ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen, 5 kap. i polislagen eller 3 kap. i lagen om brottsbekämpning inom Tullen *(623/2015)* och i vilket den som är föremål för metoden *för inhämtande av information eller åtgärder* inte behöver höras vid behandlingen av yrkandet på metoden *eller åtgärder, eller*	En parts rätt enligt 1 mom. gäller inte 1) information som avses i 11 § 2 mom. 7 och 7 a-punkten i lagen om offentlighet i myndigheternas verksamhet, 2) rättegångshandlingar som upprättats vid en domstol, före den tidpunkt som avses i 8 §, 3) ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen, 5 kap. i polislagen eller 3 kap. i lagen om brottsbekämpning inom Tullen *eller som gäller en metod för underrättelseinhämtning enligt 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik eller lagen om militär underrättelseverksamhet* och i vilket den som är föremål för metoden inte behöver höras vid behandlingen av yrkandet på metoden, *3 a) ett ärende som gäller ett i 15 § i lagen om övervakning av underrättelseverksamheten avsett interimistiskt förordnande av underrättelseombudsmannen, eller*
4) rättegångshandlingar till den del de innehåller uppgifter om domstolens överläggning.	4) rättegångshandlingar till den del de innehåller uppgifter om domstolens överläggning.
16 §	16 §
Offentligheten i tvångsmedelsärenden	*Offentligheten i tvångsmedelsärenden*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen eller enligt 5 kap. i polislagen eller tullåtgärder enligt 20 f § i tullagen och i vilket den som är föremål för metoden för inhämtande av information eller åtgärder inte behöver höras vid behandlingen av yrkandet på metoden *eller åtgärder*, handläggs och avgörandet avkunnas utan att allmänheten är närvarande. Den rättegångshandling som innehåller avgörandet samt övriga rättegångshandlingar i ärendet blir offentliga när den som misstänks för brott eller är föremål för metoden *för inhämtande av in-*	Ett ärende som gäller en hemlig metod för inhämtande av information enligt 10 kap. i tvångsmedelslagen, 5 kap. i polislagen eller *3 kap. i lagen om brottsbekämpning inom Tullen eller som gäller en metod för underrättelseinhämtning enligt 5 a kap. i polislagen, lagen om civil underrättelseinhämtning avseende datatrafik eller lagen om militär underrättelseverksamhet och i vilket den som är föremål för metoden* inte behöver höras vid behandlingen av yrkandet på metoden*,* handläggs och avgörandet avkunnas utan att allmänheten är närvarande. Den rättegångshandling som innehåller avgörandet samt öv-

Gällande lydelse

formation eller åtgärder senast ska underrättas om att sådana använts. Om personen i fråga underrättas om användningen av metoden *eller åtgärder* senare när hans eller hennes identitet är utredd, blir rättegångshandlingarna offentliga när domstolen informeras om underrättelsen. Domstolen får av särskilda skäl besluta att en rättegångshandling ska bli offentlig tidigare.

Föreslagen lydelse

riga rättegångshandlingar i ärendet blir offentliga när den som misstänks för brott eller är föremål för metoden *senast ska underrättas om att metoden* använts. Om personen i fråga underrättas om användningen av metoden senare när hans eller hennes identitet är utredd, blir rättegångshandlingarna offentliga när domstolen informeras om underrättelsen. Domstolen får av särskilda skäl besluta att en rättegångshandling ska bli offentlig tidigare.

Ett ärende som gäller ett i 15 § i lagen om övervakning av underrättelseverksamheten avsett interimistiskt förordnande av underrättelseombudsmannen handläggs och avgörandet avkunnas utan att allmänheten är närvarande. I fråga om tidpunkten för när den rättegångshandling som innehåller avgörandet samt övriga rättegångshandlingar i ärendet blir offentliga tillämpas 4 mom.

Denna lag träder i kraft den 20 .
