**RP 203/2017 rd**

**Regeringens proposition till riksdagen med förslag till lag om militär underrättelseverksamhet och till vissa lagar som har samband med den**

## PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att det stiftas en lag om militär underrättelseverksamhet. Propositionen hänger samman med regeringens proposition med förslag till lagstiftning om civil underrättelseverksamhet och tillsyn över militär underrättelseverksamhet och en revision av grundlagen så att skyddet för hemligheten i fråga om förtroliga meddelanden kan begränsas för att trygga den nationella säkerheten från sådan militär verksamhet och annan verksamhet som allvarligt hotar den. Syftet med propositionen är att uppdatera den lagstiftning som gäller Försvarsmaktens underrättelseverksamhet samt att uppfylla de krav som följer av grundlagen och internationella förpliktelser som binder Finland.

Målet är att förbättra informationsinhämtningen om allvarliga internationella hot som anknyter till Försvarsmaktens uppgifter på så sätt att Försvarsmakten inom landet och utomlands ska ha befogenheter för underrättelseinhämtning som avser person, underrättelseinhämtning som avser datasystem och underrättelseinhämtning som avser datatrafik.

Avsikten med den militära underrättelseinhämtningen är att följa med utvecklingen i den säkerhetspolitiska omgivningen och producera information om läget som stöd för den högsta säkerhetspolitiska ledningen och det militära beslutsfattandet. Den militära underrättelseinhämtningen ger en förvarning om militära hot som riktar sig mot Finland och utgör ett stöd för andra myndigheter. Dessutom stöder den militära underrättelseinhämtningen den övriga internationella verksamhet som Försvarsmakten utövar och det beslutsfattande som gäller internationella insatser samt Försvarsmaktens verksamhet och egenskydd

Det föreslås att det i lagen ska föreskrivas om föremålen för militär underrättelseverksamhet och om de principer som ska följas i underrättelseverksamheten samt om styrningen och övervakningen av verksamheten inom försvarsförvaltningen. Försvarsmaktens huvudstab och Försvarsmaktens underrättelsetjänst är militärunderrättelsemyndigheter enligt förslaget. Det föreskrivs i lagen om de underrättelsemetoder som står till myndigheternas förfogande och om beslutsfattandet om utövandet av befogenheterna samt om samarbete med andra myndigheter, anmälan om en underrättelseuppgift, förbud mot underrättelseinhämtning och internationellt samarbete.

I propositionen föreslås det dessutom att lagen om försvarsmakten, lagen om verksamheten i den offentliga förvaltningens säkerhetsnät och inkomstskattelagen ska ändras. Lagen om militär disciplin och brottsbekämpning inom försvarsmakten ändras på grund av den proposition med förslag till lagstiftning om civil underrättelseinhämtning som överlämnats till riksdagen och enligt vilken skyddspolisen ska avstå från sina förundersökningsbefogenheter.

Den föreslagna lagen ska träda i kraft så snart som möjligt med beaktande av de omständigheter som gäller den föreslagna lagens lagstiftningsordning.

———

**INNEHÅLL**

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL ..... 1
INNEHÅLL ..... 2
ALLMÄN MOTIVERING ..... 5
1 INLEDNING ..... 5
2 NULÄGET ..... 6
2.1 En föränderlig säkerhetspolitisk omgivning ..... 6
2.2 Lagstiftning och praxis ..... 11
2.2.1 Lagstiftning om Försvarsmakten och informationsanskaffning ..... 11
2.2.2 Nuläget i fråga om informationsinhämtningen inom Försvarsmakten ..... 19
2.2.3 Hemliga metoder för inhämtande av information ..... 20
2.2.4 Allmänt om hemliga metoder för inhämtande av information ..... 22
2.2.5 Försvarsmaktens andra metoder för inhämtande av information ..... 33
2.2.6 Försvarsmaktens informationsinhämtning utomlands ..... 36
2.2.7 Styrning av Försvarsmakten ..... 37
2.2.8 Ordnandet av militär underrättelseinhämtning ..... 37
2.2.9 Värnplikt och reservister ..... 39
2.2.10 Rättslig övervakning av Försvarsmakten ..... 39
2.2.11 Bekämpning av hot mot informationssäkerhet ..... 44
2.3 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU ..... 46
2.3.1 Internationella konventioner om mänskliga rättigheter ..... 46
2.3.2 Lagstiftningen i utlandet ..... 62
2.4 Bedömning av nuläget ..... 86
2.4.1 Allmänt ..... 86
2.4.2 Föremålen för informationsinhämtning ..... 88
2.4.3 Försvarsmaktens befogenheter att inhämta information ..... 89
2.4.4 Hemliga metoder för inhämtande av information ..... 92
2.4.5 Beslutsfattande ..... 113
2.4.6 Bestämmelser som är gemensamma för alla hemliga metoder för inhämtande av information ..... 115
2.4.7 Underrättelseinhämtning som avser utländska förhållanden ..... 121
2.4.8 Styrning och tillsyn ..... 124
2.4.9 Rättslig övervakning och rättsskydd ..... 125
2.4.10 Utlämnande av uppgifter samt internationellt samarbete ..... 126
2.4.11 Reservisters deltagande i militär underrättelseinhämtning ..... 126
2.4.12 Organisationernas möjlighet att gardera sig mot hot mot informationssäkerheten ..... 127
2.4.13 Sammanfattning av bedömningen av nuläget ..... 127
3 MÅLSÄTTNING OCH DE VIKTIGASTE FÖRSLAGEN ..... 129
3.1 Målsättning ..... 129
3.2 Alternativ ..... 131
3.2.1. Bevarande av nuläget och nykriminaliseringar ..... 131
3.2.2 Förslag av arbetsgruppen för en informationsanskaffningslag ..... 134

3.2.3 Förslag av arbetsgruppen för en lag om militär underrättelseverksamhet....135
3.2.4 Bedömning av alternativen....139
3.3 De viktigaste förslagen....142
4 PROPOSITIONENS KONSEKVENSER....155
4.1 Ekonomiska konsekvenser....155
4.1.1 Konsekvenser för de offentliga finanserna....155
4.1.2 Konsekvenser för samhällsekonomin och för företag....160
4.1.3 Konsekvenser för myndigheterna....163
4.1.4 Konsekvenser för hushållens ställning....166
4.2 Samhälleliga konsekvenser....167
4.2.1 Medborgarnas ställning i samhället och verksamheten i det civila samhället....167
4.2.2 Konsekvenser för brottsbekämpningen och säkerheten....168
4.2.3 Konsekvenser för informationssamhället....169
4.3 Jämförelse av för- och nackdelar....173
4.3.1 Avvärjande av hot mot det militära försvaret och den nationella säkerheten....173
4.3.2 Brottsbekämpning....174
4.3.3 Tillgodoseende av de grundläggande fri- och rättigheterna....174
4.3.4 Direkta kostnadseffekter....174
4.3.5 Slutsatser....174
5 BEREDNINGEN AV PROPOSITIONEN....174
5.1 Beredningsskeden och beredningsmaterial....174
5.2 Remissyttranden och hur de har beaktats....176
5.2.1 Ekonomiska konsekvenser....176
5.2.2 Förhållande till grundlagen samt lagstiftningsordning....177
5.2.3 Föremål för den militära underrättelseinhämtningen....177
5.2.4 Utlämnande av uppgifter i vissa situationer....177
5.2.5 Förundersökning....177
5.2.6 Behandling av personuppgifter....178
5.2.7 Utlåtande av rådet för bedömning av lagstiftningen....178
6 ÅLANDS STÄLLNING....180
7 SAMBAND MED ANDRA PROPOSITIONER....181
DETALJMOTIVERING....183
1 LAGFÖRSLAG....183
1.1 Lagen om militär underrättelseverksamhet....183
1 kap. Allmänna bestämmelser....183
2 kap. Styrning av och tillsyn över den militära underrättelseinhämtningen....214
3 kap. Samverkan med andra myndigheter och internationellt samarbete....219
4 kap. Metoder för underrättelseinhämtning....225
5 kap. Skyddande av militär underrättelseinhämtning samt tryggande av tjänstemän och informationskällor....308
6 kap. Utlämnande av underrättelseuppgifter i vissa fall....313

7 kap. Förbud mot underrättelseinhämtning, utplåning av underrättelseinformation och underrättelse om användning av en metod för underrättelseinhämtning ..... 319
8 kap. Försvarsmaktens tjänstemäns och värnpliktigas deltagande i militär underrättelseinhämtning samt internationell verksamhet ..... 333
9 kap. Yppandeförbud, skyldigheter och rättigheter som gäller teleföretag och dataöverförare samt användning och erhållande av information ..... 336
10 kap. Övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen ..... 344
11 kap. Särskilda bestämmelser ..... 346
1.2 Lagen om försvarsmakten ..... 354
1.3 Lagen om militär disciplin och brottsbekämpning inom försvarsmakten ..... 354
1.4 Lagen om verksamheten i den offentliga förvaltningens säkerhetsnät ..... 356
1.5 Inkomstskattelagen ..... 357
2 Närmare bestämmelser och föreskrifter ..... 358
3 Ikraftträdande ..... 358
4 Förhållande till grundlagen och lagstiftningsordning ..... 360
4.1 Inledning ..... 360
4.2 Förslagen till bestämmelser om metoder för underrättelseinhämtning med hänsyn till bestämmelserna om de grundläggande fri- och rättigheterna ..... 361
4.3 De övriga lagförslagens förhållande till grundlagen ..... 372
4.4 Bedömning av propositionen med avseende på Europadomstolens avgörandepraxis ..... 376
4.5 Bedömning av lagstiftningsordningen ..... 379
Lagförslag ..... 380
Lag om militär underrättelseverksamhet ..... 380
Lag om ändring av lagen om försvarsmakten ..... 421
Lag om ändring av lagen om militär disciplin och brottsbekämpning inom försvarsmakten ..... 422
Lag om ändring av 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät ..... 424
Lag om ändring av 92 b § i inkomstskattelagen ..... 425
BILAGOR ..... 426
PARALLELLTEXT ..... 426
Lag om ändring av lagen om militär disciplin och brottsbekämpning inom försvarsmakten ..... 426
Lag om ändring av 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät ..... 429
Lag om ändring av 92 b § i inkomstskattelagen ..... 430

## ALLMÄN MOTIVERING

### 1 Inledning

Den allmänna utvecklingen mot en allt större internationalisering och teknifiering är viktig och oundgänglig. Till följd av detta har Finlands säkerhetspolitiska omgivning förändrats avsevärt under de senaste åren, samtidigt som den blivit allt mer komplicerad. Dessutom överlappar de hot som riktas mot den interna och externa säkerheten varandra i allt större utsträckning. De allvarligaste hoten mot vår säkerhet har nästan alltid internationellt ursprung eller utomstående kopplingar. Också Finlands intressen utomlands – inklusive sådana krishanteringsinsatser där Finland deltar –blir mer och mer utsatta för allt allvarligare hot. Det har blivit svårare att känna igen de stater och icke-statliga aktörer som står bakom hoten och att förebygga dem, eftersom t.ex. den tekniska och informationstekniska utvecklingen har gett också små stater och andra aktörer möjlighet till effektiv verksamhet. Utvecklingen på det tekniska området har gjort det möjligt att genomföra handlingar som hotar den nationella säkerheten med mycket kortare förberedelser och med mycket allvarligare följder. Cyberattacker kan också användas som verktyg för politisk och ekonomisk påtryckning och kan vid allvarliga kriser användas som en påverkningsmetod vid sidan av traditionella militära maktmedel.

Av hotens internationella karaktär följer att de aktörer som står bakom dem har bildat nätverk på olika länders territorium och att parterna kommunicerar över nationsgränserna. Den snabba utvecklingen inom kommunikationstekniken har effektiviserat och underlättat kontakterna och nätverksbildandet över gränserna mellan de aktörer som hotar Finland samtidigt som dessa faktorer har påskyndat internationaliseringen av hoten. Utvecklingen har påverkats av att väpnade styrkor på grund av den snabba informationstekniska utvecklingen och lägre kostnader i stor omfattning tar i bruk sådana lednings- och kommunikationssystem som ursprungligen var planerade för civila ändamål. Vid sidan av civila aktörer stöder också moderna stridskrafter sig allt mer på den allmänna teleinfrastrukturen. För den tekniska utvecklingens vidkommande är det viktigt att notera att också den datatrafik som stridskrafterna utnyttjar i stor utsträckning har övergått från analoga till digitala kanaler, såsom kablar för telekommunikation.

De utmaningar som sammanhänger med den säkerhetspolitiska omgivningen och gränsöverskridande hot är allt mer mångfasetterade. För att myndigheterna ska kunna svara på dessa utmaningar och hot krävs det att de har tillgång till och utvecklar en allt bredare metodarsenal. Upprätthållandet av säkerheten kräver en aktiv utrikes-, säkerhets- och försvarspolitik. Behovet av samverkan mellan de olika politikområdena för inre och yttre säkerhet accentueras. Det krävs ett brett och intensivt samarbete på nationell nivå, EU-nivå och internationell nivå för att vi ska kunna stå upp mot hotbilderna. Lissabonfördaget (FördrS 66 och 67/2009), som trädde i kraft 2009, har stärkt EU:s roll när det gäller att möta olika hot. EU:s solidaritetsklausul (artikel 222 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget)) och klausul om ömsesidigt bistånd (artikel 42.7 i fördraget om Europeiska unionen (FEU)) framhäver unionens karaktär av säkerhetsgemenskap och förbättrar EU-medlemsstaternas möjligheter att begära och ge varandra bistånd i olika krissituationer.

De myndigheter som svarar för den nationella säkerheten har till uppgift att föregripa och förebygga sådana handlingar och åtgärder som kan äventyra de nationella intressen som upplevs som särskilt viktiga. Allvarliga hot mot Finlands säkerhet kan också riktas mot landet utifrån. De allt mer utvecklade datanäten har minskat de fysiska avståndens betydelse för verkställandet av hoten. De myndigheter som svarar för den nationella säkerheten bedriver sådan underrättelseinhämtning som behövs för att de ska kunna sköta sina lagfästa uppgifter. Det finns emellertid inte några lagfästa befogenheter för inhämtning av underrättelser. Underrättelsein-

hämtningen grundar sig till stor del på officiella källor och på den information som fås inom ramen för internationellt och frivilligt samarbete.

Försvarsmakten, som hör till försvarsministeriets förvaltningsområde, svarar för Finlands militära försvar och för landets beredskap inför militära hot. Förvaltningsområdets behov av informationsinhämtning ansluter sig till formandet och upprätthållandet av en militärstrategisk lägesbild och till säkerheten när det gäller internationella uppdrag. För att Försvarsmakten ska kunna utföra sina lagfästa uppgifter krävs tillgång till ett system för militär underrättelseinhämtning som kan användas för att följa utvecklingen i den säkerhetspolitiska omgivningen och kännedom om den operativa verksamhetsomgivningen och bedömningar av den till stöd för de beslut som statens och Försvarsmaktens ledning ska fatta. Systemet ger statsledningen en förvarning om militära hot under uppsegling, vilket gör det möjligt att fatta rättidiga beslut och leda samhällets vitala funktioner. I den militära underrättelseverksamheten framhävs därmed kapaciteten för tidig förvarning, alltså förmågan att förvarna om eventuella militära hot för att inta beredskap att svara på dem.

Med militär underrättelseverksamhet avses riktad informationsinhämtning och analysering av den information som inhämtats i den rådande säkerhetspolitiska omgivningen samt olika aktörers aktionsberedskap och planer i syfte att framställa information till stöd för statens högsta lednings och Försvarsmaktens beslutsfattande.

Enligt regeringsprogrammet för statsminister Juha Sipiläs regering (SRM 1/2015 rd) kräver de ökande riskerna och nya hot beredskap och förberedelser av ett helt nytt slag av hela samhället. Regeringen ska stärka arbetet för det övergripande säkerhetstänkandet såväl nationellt som inom EU och i internationellt samarbete. Detta gäller framför allt nya och omfattande hot såsom hybridpåverkan, cyberattacker och bekämpning av terrorism. Regeringen fastställer interna villkor för den yttre säkerheten. Regeringen lägger fram rättsliga grunder för underrättelse utomlands och för datatrafikspaning. I detta sammanhang ska man beakta tillgodoseendet av de grundläggande fri- och rättigheterna och de mänskliga rättigheterna.

Projektet för underrättelselagstiftning behandlades vid regeringens strategimöte den 20 augusti 2015. Vid mötet beslutades det att försvarsministeriet ska leda ett projekt för militär underrättelseverksamhet, inrikesministeritet ett projekt för civil underrättelseverksamhet och justitieministeriet ett projekt för en eventuell ändring av grundlagen. Försvarsministeriet tillsatte den 1 oktober 2015 ett projekt med uppgift att bereda ett förslag till lagstiftning om militär underrättelseverksamhet. Lagstiftningen bereddes i nära samarbete med inrikesministeriet och justitieministeriet inom ramen för de olika projekten. Justitieministeriet inledde den 17 oktober 2016 ett projekt för ordnande av tillsyn över säkerhetsmyndigheternas underrättelseverksamhet.

## 2 Nuläget

### 2.1 En föränderlig säkerhetspolitisk omgivning

Statsrådet lämnade den 19 maj 2016 en redogörelse för den inre säkerheten (SRR 5/2016 rd) och den 17 juni 2016 en utrikes- och säkerhetspolitisk redogörelse (SRR 6/2016 rd) till riksdagen. Bägge redogörelserna utgår på det sätt som förutsätts i regeringsprogrammet från begreppet övergripande säkerhet. Statsrådets försvarspolitiska redogörelse lämnades till riksdagen den 16 februari 2017 (SRR 5/2017 rd). Redogörelsen för den inre säkerheten, den utrikes- och säkerhetspolitiska redogörelsen och den försvarspolitiska redogörelsen bildar den centrala referensramen för den övergripande säkerheten och granskningsperioderna för redogörelserna

sträcker sig fram till medlet av 2020-talet. Bakgrunden till arbetet utgjordes av den säkerhets- och försvarspolitiska redogörelsen från 2012 och säkerhetsstrategin för samhället från 2010.

Enligt den försvarspolitiska redogörelsen har säkerhetsläget i Finlands närområde blivit sämre efter erövringen av Krim och genom den pågående konflikten i östra Ukraina. De militära spänningarna i Östersjöområdet har ökat och osäkerheten har brett ut sig också mer allmänt.

Östersjöområdet har fått större militärstrategisk betydelse och den militära aktiviteten i området har ökat. Det har visat sig att Ryssland kan fatta strategiska beslut snabbt och även använda militära maktmedel och annan omfattande metodarsenal samordnat för att nå sina mål. Landet utvecklar sina väpnade styrkors operativa förmågor och upprätthåller färdigheterna att agera också i en storskalig militär kris. De trupper som står i hög beredskap inom alla försvarsgrenar kan snabbt och överraskande flyttas från olika delar av landet i önskad riktning bland annat för att erövra ett begränsat område och bestrida målstatens suveränitet. Alla Rysslands säkerhetsmyndigheters operativa förmågor kan användas för militära uppdrag. Eftersom bilden av kriget har blivit mer komplex, är utbudet av de medel som kan riktas mot Finland under en kris vidsträckt. Detta utbud inbegriper både militära och icke-militära medel. Tiden för förvarning vid militära kriser har blivit kortare och tröskeln för att ta till maktmedel har sänkts. Samtidigt har samhället blivit mera sårbart.

Enligt den försvarspolitiska redogörelsen ökar cyberomgivningens betydelse. Det går inte att utesluta att cybermetoder kan användas för att uppnå politiska mål. Digitaliseringen av samhället, de tekniska systemens beroende av gränsöverskridande datanät samt systemens ömsesidiga beroendeförhållanden och sårbarheter gör samhällets vitala funktioner mottagliga för cyberpåverkan. I våra närområden och även i Finland har cyber- och informationspåverkan riktats mot bl.a. kritisk infrastruktur, industriinrättningar samt det politiska beslutssystemet och medborgarna. Utvecklingen inom vetenskap och teknik orsakar också utmaningar av andra slag när det gäller att bereda sig på hot. Mångfalden av kemiska, biologiska och radiologiska hot och kärnvapenhot (CBRN) kvarstår.

Enligt den försvarspolitiska redogörelsen från 2017 stärker Finland sin nationella försvarsförmåga och intensifierar sitt internationella försvarssamarbete genom att bygga upp nya förmågor i cyberomgivningen.

Enligt redogörelsen förutsätts förmåga att agera både på marken, till sjöss, i luften och i cyberomgivningen för att Finland ska kunna försvaras. De krav som verksamhetsmiljön ställer framhäver bl.a. spaningsförmåga, förvaltningsområdenas beredskap att agera i situationer som utvecklas snabbt, förmåga att skydda sig mot verkningar av vapensystem med lång räckvidd och cyberförsvarsförmåga.

Enligt redogörelsen för den inre säkerheten överlappar hoten mot den inre och yttre säkerheten varandra i allt större utsträckning. Hoten blir allt mer komplicerade och förändras snabbt. Det har på senare tid blivit betydligt svårare att förutse säkerhetssituationen och någon förändring till det bättre är inte att vänta. I den uppkomna situationen framhävs den inre säkerhetens betydelse och av denna orsak gjorde statsrådet för första gången en separat redogörelse för den inre säkerheten.

Enligt den är bl.a. de försämrade relationerna mellan Ryssland och västländerna samt cyberhoten bland de viktigaste förändringarna i den säkerhetspolitiska omgivningen. Enligt redogörelsen har metoderna för hybridpåverkan ökat när det gäller att påverka stater och de myndigheter som svarar för den inre säkerheten ska kunna identifiera hot och ha tillräckliga resurser för

att hantera dem, också under en längre tid. Också informationspåverkan från andra stater och aktörer ska man kunna upptäcka och ha förmåga att reagera mot. I den situation som har uppstått betonas tryggandet av det statliga beslutsfattandet och de yttre gränsernas integritet.

Det är också möjligt att nya spänningar uppstår mellan länderna. Dessutom bedöms det att utländska underrättelsetjänster har utökat sin verksamhet. Vid sidan av den traditionella underrättelseverksamheten har underrättelseinhämtning i informationsnäten ökat. Störningar i den kritiska infrastrukturen kan påverka ett stort antal personer. Enligt redogörelsen är de element som mest påverkar den inre säkerheten bl.a. försörjningsberedskapen, digitaliseringen, cybersäkerheten och basinfrastrukturen och deras starka inbördes beroendeförhållanden.

Den utrikes- och säkerhetspolitiska redogörelsen utgör grunden för Finlands utrikes- och säkerhetspolitik. I redogörelsen behandlas de ständigt skiftande och svårförutsebara utvecklingsförloppen i den internationella omgivningen och vilken betydelse det har för landets säkerhet att säkerhetsfrågorna blir allt mer globala. Enligt redogörelsen fortsätter den kraftiga omvälvningen i den utrikes- och säkerhetspolitiska omvärlden såväl i Finlands närområden som globalt. Stater och andra aktörer har allt tätare och mer mångskiftande kopplingar och beroendeförhållanden till varandra. Förändringarna i vår omvärld den senaste tiden har också skapat nya hot och osäkerhet. Den internationella säkerhetssituationen har ur europeiskt perspektiv försvagats de senaste åren. De internationellt sett betydelsefulla aktörerna är allt fler och av skiftande slag, och maktförhållandena mellan dem förändras ständigt. Förändringarna i den utrikes- och säkerhetspolitiska omgivningen påverkar också på många sätt hur Finlands inre säkerhet utvecklas. I och med dem är den inre säkerheten föremål för nya osäkerhetsfaktorer och samhällets allmänna kristålighet sätts på prov.

Enligt den utrikes- och säkerhetspolitiska redogörelsen grundar sig de utrikes- och säkerhetspolitiska målsättningarna och det utrikes- och säkerhetspolitiska beslutsfattandet och inflytandet på information från omvärlden. Information om variablerna i omgivningen och de möjligheter och hot de ger upphov till måste kontinuerligt inhämtas och analyseras. Utifrån informationen och analyserna ska det finnas beredskap att anpassa verksamheten och vid behov förskjuta tyngdpunkten i utrikes- och säkerhetspolitiken. De viktigaste yttre variablerna i Finlands utrikes- och säkerhetspolitiska omvärld är globala utvecklingstrender, den politiska utvecklingen och säkerhetsutvecklingen i för Finland strategiska geografiska områden, de utrikes- och säkerhetspolitiska aktörerna och internationellt vedertagna normer.

Sammantaget kan man konstatera att redogörelserna framhåller att finländarnas säkerhet och välfärd måste förbättras. Avvärjandet av gränsöverskridande hot och beredskapen inför sådana förutsätter utöver utnyttjandet av såväl militära som civila resurser också ett brett metodurval. Utifrån sina egna starka sidor ska Finland kunna förutse förändringar i omgivningen och svara på de krav som förändringarna ger upphov till. En situation där finländska myndigheter på grund av bristfällig nationell lagstiftning är beroende av utländska källor för att få information om hot mot landets vitala intressen är ohållbar. Varje stat – också Finland – har en skyldighet att värna om sin egen och sina invånares säkerhet och att grunda sina beslut om landets säkerhet på information som staten själv har inhämtat.

*Den nationella säkerhetspolitiska omgivningen*

Enligt säkerhetsstrategin för samhället från 2010 kan statens självbestämmanderätt anses vara ett av de viktigaste intressena för landet att skydda. Med statens självbestämmanderätt avses suveränitet i förhållande till främmande makter och rätt att inom det egna landets gränser utöva den högsta makten utan inblandning av andra. Bland andra intressen som det är viktigt att

värna om kan man räkna åtminstone statens ledning, internationell verksamhet, försvarsförmåga, inre säkerhet, fungerande ekonomi och infrastruktur och befolkningens utkomstskydd och funktionsförmåga. Hot mot dessa intressen kan anses äventyra nationens säkerhet. De myndigheter som svarar för avvärjandet av hoten kallas nationella säkerhetsmyndigheter. I och med globaliseringen har gränserna mellan staternas yttre och inre säkerhet blivit allt mer flytande. Det har också blivit allt svårare att avgränsa hoten och riskerna som regionala eller lokala på grund av att ekonomiska, tekniska och sociala system är gränsöverskridande och beroende av varandra. De faktorer som utgör de största hoten mot landets säkerhet anknyter numera ofta till händelser utanför landets gränser. Det blir därmed allt mera sannolikt att följderna av olika hot med utländskt ursprung eller som uppkommer utomlands kan realiseras i vårt land. Det gemensamma för yttre hot mot den nationella säkerheten är att det blir allt svårare att identifiera de statliga och icke-statliga aktörer som ligger bakom dem och särskilja mellan dem. Av denna anledning är det svårare än tidigare att föregripa hoten.

Också de militära hoten har ändrat karaktär. Utöver de traditionella militära aktiviteterna omfattar de moderna militära insatserna olika asymmetriska metoder. Nuförtiden inleds militära insatser tidsmässigt redan under fredstid med påtryckning och desinformation samt cyberattacker. På så sätt kan en främmande aktör medvetet försöka påverka beslutsfattandet i en annan stat för att nå sådana strategiska mål som staten i fråga inte annars skulle gå med på. Numera ingår påtrycknings- och desinformationskampanjer bland de åtgärder staterna använder i sin utrikes- och säkerhetspolitik. Samtidigt har de icke-statliga aktörernas påverkningsmöjligheter vid militära insatser ökat i och med att tekniken har utvecklats och samhällenas sårbarhet ökat.

Gränsen mellan politisk påverkan och krigföring blir flytande när politiska och ekonomiska påtryckningsmetoder och desinformationskampanjer utnyttjas. I framtiden betyder inte ens omfattande användning av maktmedel nödvändigtvis att man tar stora landområden i besittning eller tar kontroll över sådana. Man kan i stället försöka nå sina mål genom överraskande bruk av militärt våld och genom snabb erövring av begränsade områden.

*Ett samhälle allt mer beroende av informationsteknik*

Människan söker numera till största delen information och umgås via nätet. Samhället har övergått till att bli en miljö där nästan alla traditionella tjänster och aktiviteter styrs av informationsteknik eller helt och hållet sker i informationsnät. Den logik som styr informationsnäten skiljer sig från den som gällde i de gamla telefonnäten. När ett telefonsamtal helt och hållet förbehöll det kretsförmedlade telefonnätet för parterna i samtalet, den som ringde upp och den som blev uppringd, löper trafiken i internet kors och tvärs mellan flera uppkopplingar. Den avsändande enheten delar upp meddelandet i IP-paket som den mottagande enheten sätter ihop igen till ett helt meddelande. Alla paket tar inte nödvändigtvis samma rutt till mottagare, eftersom nätet styr varje paket till en rutt som just för ögonblicket är den mest kostnadseffektiva. Datakommunikationen mellan två parter som befinner sig i samma land kan förmedlas via en utländsk knutpunkt.

Vidareutvecklingen av datanäten har gjort att t.ex. molntjänster har blivit vanligare. Molntjänster är en form av tjänster för datalagring som gör det möjligt för den som innehar rättigheterna till informationen att få tillgång till den från vilken anordning som helst som är uppkopplad till nätet. De servrar som sköter molntjänsterna kan vara placerade på en eller flera staters territorium. Användaren har inte nödvändigtvis möjlighet att få reda på var informationen fysiskt är placerad.

Hot mot säkerheten sammanhänger i och med globaliseringen allt oftare med kopplingar mellan personer i Finland och personer utomlands och det behov av ömsesidig kommunikation som blir konsekvensen. Elektroniska verktyg används i kommunikationen mellan de statliga och icke-statliga aktörer som står bakom säkerhetshoten, i rapporteringen över hur ett givet uppdrag har genomförts, planeringen av uppdrag, inhämtandet av information om föremålen för uppdragen och för att motivera och radikalisera deltagarna och rekrytera nya medlemmar. En förutsättning för att avvärja hoten på ett framgångsrikt sätt är att de myndigheter som ansvarar för den nationella säkerheten i ett så tidigt skede som möjligt får vetskap om detta slag av förbindelser och de omständigheter som kan äventyra den nationella säkerheten inom ramen för förbindelserna.

Tillgång till information i ett tidigt skede förbättrar det finländska samhällets möjligheter till respons och breddar den metodarsenal som står till buds för att förhindra eller inta beredskap inför realiseringen av hoten. Den information om kommunikationen i datanät som myndigheter ansvariga för nationens säkerhet har inhämtat har globalt sett intagit en central ställning när det gäller att förhindra sådana gärningar.

Det kommer att bli ännu viktigare bland aktörer som hotar nationens säkerhet av att bilda nätverk med hjälp av datanät. I och med utvecklingen av sociala medier blir sätten att bilda nätverk ännu fler. Statliga aktörer satsar på att utveckla egna moderna medieorganisationer och sprida propaganda via dem. De använder i allt större utsträckning sociala medier, såsom snabba meddelandetjänster, och upprätthåller öppna och slutna diskussionsforum. Dessa möjliggör inte bara lättanvända kommunikationskanaler mellan två eller flera användare, utan också att planeringen och samordningen av verksamheten kan ske i realtid.

Främmande makters målsystem har blivit mer komplicerade, mängden signaler har ökat avsevärt och en allt större del av datakommunikationen förmedlas i stället för med hjälp av radio med hjälp av telekommunikationskablar. På grund av denna förändring i omvärlden har Finlands militära underrättelseinhämtning sämre möjligheter att samla in underrättelseinformation. Ledningen av stridskrafterna stöder sig allt mer på den allmänna datanätsinfrastrukturen. För att vara effektiv i en omvärld där informationstekniken tar allt större plats bör dagens underrättelseinhämtning fokusera också på digital information.

*Hot som riktas mot Finland via informationsnätet*

Digitaliseringens inverkan på hur den säkerhetspolitiska miljön utvecklas och på cybersäkerheten tas upp 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 informationsanskaffning) från 2015.

Det konstateras i strategin för cybersäkerheten att Finland som informationssamhälle är beroende av funktioner i datanät och IT-system och landet är således också mycket sårbart för störningar som riktas mot dessa. De hot som riktas mot cyberomgivningen har blivit mycket farligare med avseende på vilka effekter de kan få får enskilda, företag och samhället i stort. De aktörer som står bakom hoten är mer professionella än tidigare och numera kan också statliga aktörer räknas till dem. I en cyberomgivning kan attacker också användas som verktyg för politisk och ekonomisk påtryckning och kan vid allvarliga kriser användas som en påverkningsmetod vid sidan av traditionella militära maktmedel.

Betänkandet av försvarsministeriets arbetsgrupp för informationsanskaffning tar upp digitaliseringens effekter ur såväl ett kommunikationsperspektiv som med utgångspunkt i hoten mot

informationsnäten. I kommunikationshänseende gör digitaliseringen det möjligt för de aktörer som hotar nationens säkerhet att bilda nätverk i väsentligt större omfattning och på ett mer mångsidigt sätt. Informationsnätet utnyttjas bland dessa aktörer som ett medel för att kommunicera om sådana planer och intentioner som gäller gärningar i världen utanför. Gärningarna kan vara militära till sin natur (väpnat angrepp) eller rikta sig mot andra nationella intressen, såsom statens territoriella integritet, t.ex. i form av spionage. Informationsnäten kan också utnyttjas som egentliga medel för att rikta gärningar mot föremålet för informationsinhämtningen, t.ex. staten Finland, för att åstadkomma allvarliga skador. Det kan då vara fråga om det som i cybersäkerhetsstrategin beskrivs som cyberspionage eller cyberattacker.

De aktörer som utgör ett hot mot landets försvar och nationens säkerhet använder informationsnäten inte bara för kommunikation utan också som ett verktyg för att verkställa hoten. Enligt säkerhetsmyndigheternas bedömning strävar många främmande stater efter att rikta ett omfattande och tekniskt avancerat cyberspionage mot Finlands statsförvaltning och mot företag som är nationalekonomiskt sett viktiga.

Sådana hot mot statens livskraft eller hot som kan äventyra statens vitala säkerhetsintressen som tas upp i strategin är framför allt cyberspionage, cyberterrorism och cyberinsatser. Det sistnämnda innefattar såväl påtryckningar som konflikter på en nivå näst intill krigföring i cyberomgivningen, men också cyberinsatser som anknyter till krig. Genom cyberspionage skaffas information i stil med stats- eller företagshemligheter eller känslig information som finns i informationssystemen. Spionage i cyberomgivningen kan pågå obemärkt i flera år. Utöver program för underrättelseinhämtning kan sabotageprogram införas i informationssystemen och aktiveras när en kris börjar. Ny teknik skapar nya möjligheter att bedriva krigföring genom cyberinsatser vars konsekvenser drabbar hela samhället, inte enbart de väpnade styrkorna.

Cyberspionaget och cyberinsatserna får allt större betydelse under de kommande åren. Orsaken till detta är att dåd i cyberomgivningen kan genomföras till låga kostnader, att det är svårt och dyrt att skydda sig mot dem och att risken att ertappas är liten. Alla de främmande makter som är av betydelse för utvecklingen i Finlands säkerhetspolitiska omgivning satsar också målmedvetet på att bygga ut sin offensiva cyberkapacitet. Som exempel på cyberinsatser kan nämnas nätintrång i slutna myndighetnätverk i bl.a. Ukraina (2014), Georgien (2008) och Estland (2007), vilka alla har visat sig vara välorganiserade och välplanerade insatser där en statlig aktör, eller aktörer med mycket nära koppling till en stat, bedöms stå bakom insatserna.

Statsrådets kansli publicerade den 17 februari 2017 en oberoende undersökning om cybersäkerhetens tillstånd i Finland (Publikationsserien för statsrådets utrednings- och forskningsverksamhet 30/2017). Enligt undersökningen finns det brister i förmågan att upptäcka olika incidenter med anknytning till cybersäkerheten. Lägesuppfattningen är därför dålig och förutsättningarna för att förhindra, begränsa och återhämta sig från allvarliga cyberattacker är begränsad. För närvarande är inte alla de livsviktiga funktionerna i det finländska samhället och alla de företag som är kritiska för försörjningsberedskapen skyddade i tillräcklig grad mot olika cyberhot, och en del av de objekt som bör skyddas har fortfarande bristande resiliens (förmåga att stå emot störningar). Man har inte lyckats uppdatera Finlands lagstiftning på ett sätt som motsvarar de krav cybersäkerheten ställer. En modernisering av lagstiftningen om underrättelseverksamhet bedöms vara nödvändig för att förbättra förmågan att upptäcka incidenter och hot.

## 2.2 Lagstiftning och praxis

### 2.2.1 Lagstiftning om Försvarsmakten och informationsanskaffning

*Lagen om försvarsmakten*

Enligt 2 § i lagen om försvarsmakten (551/2007) hör det militära försvaret, stödjandet av andra myndigheter och deltagandet i militär krishantering till Försvarsmaktens uppgifter. Till det militära försvaret av Finland hör enligt 2 § 1 mom. 1 punkten underpunkt a övervakning av landområdena, vattenområdena och luftrummet samt tryggande av den territoriella integriteten och enligt 2 § 1 mom. 1 punkten underpunkt b tryggande av befolkningens livsbetingelser, de grundläggande fri- och rättigheterna och statsledningens handlingsfrihet samt försvar av den lagliga samhällsordningen.

I detaljmotiveringen till 2 § (RP 264/2006 rd) konstateras det att underrättelse- och övervakningssystemet måste följa upp utvecklingen inom Finlands säkerhetsmiljö, fastställa förändringar i miljön och producera information om den rådande situationen för att skapa och upprätthålla en militärstrategisk lägesbild. Systemet ger en förvarning om att militära hot håller på att utvecklas, så att behövliga motåtgärder kan inledas.

I en ändring av lagen om försvarsmakten (427/2017) infördes en fjärde lagfäst uppgift för försvarsmakten, nämligen deltagande i stöd och bistånd som grundar sig på artikel 222 i fördraget om Europeiska unionens funktionssätt eller artikel 42.7 i fördraget om Europeiska unionen samt deltagande i territorialövervakningssamarbete eller i annat internationellt bistånd och annan internationell verksamhet. EU:s solidaritetsklausul och klausulen om ömsesidigt bistånd framhäver unionens karaktär av säkerhetsgemenskap och förbättrar EU-medlemsstaternas möjligheter att begära och ge varandra bistånd i olika krissituationer. I och med författningsändringen kan Finland fullt ut delta i ett samarbete i enlighet med landets internationella åtaganden och i situationer som kräver att bistånd ges eller begärs och som berör försvarsministeriets förvaltningsområde.

Enligt 31 § i lagen om försvarsmakten beslutar republikens president om de centrala grunderna för rikets militära försvar, om betydande ändringar i den militära försvarsberedskapen, om principerna för genomförande av det militära försvaret samt om andra vittsyftande eller principiellt viktiga militära kommandomål som gäller försvarsmaktens militära verksamhet och militära ordning. Förfarandet för kommandomål har betydelse för tilldelningen av underrättelseuppdrag.

Det finns inte några bestämmelser om befogenheter för militär underrättelseverksamhet. Däremot finns det bestämmelser om kontraspionage, dvs. förebyggande och avslöjande av underrättelseverksamhet på finskt territorium som äventyrar syftet med det militära försvaret, i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014).

*Lagen om militär krishantering*

Enligt 2 § 1 mom. 4 punkten i lagen om försvarsmakten är en av Försvarsmaktens uppgifter att delta i internationell militär krishantering. I 2 kap. i lagen föreskrivs det om Försvarsmaktens behörighet. Enligt 13 § deltar Försvarsmakten i internationell militär krishantering i enlighet med vad som föreskrivs i lagen om militär krishantering (211/2006).

Enligt 5 § i lagen om militär krishantering ger försvarsministeriet Försvarsmakten de uppdrag som den militära krishanteringen förutsätter samt styr och övervakar den militära krishanteringen. Enligt lagen kan den finländska krishanteringsorganisationen omfatta krishanteringsstyrkor, avdelta enheter och enskilda personer. Krishanteringsorganisationen hör till Försvarsmakten och är underställd Huvudstaben på det sätt som bestäms i 5 § lagen. I operativt

hänseende är krishanteringsorganisationen underställd den föranstaltare som avses i 1 § 3 mom. i lagen. Dessa kan vara FN, Organisationen för säkerhet och samarbete i Europa (OSSE), Europeiska unionen (EU) eller någon annan internationell organisation eller grupp av länder. Det finns inte några särskilda bestämmelser om militär underrättelseverksamhet under krishanteringsinsatser i vare sig lagen om militär krishantering eller lagen om försvarsmakten.

Enligt 7 § 1 mom. i lagen om militär krishantering avses med krishanteringspersonal personer som ingått tjänstgöringsförbindelse enligt 8 § 1 mom., personer som hör till krishanteringsorganisationen, utbytespersonal samt personer som särskilt förordnas till uppgifter som gäller beredning och beredskap.

Enligt 7 § 2 mom. står krishanteringspersonalen efter att tjänstgöringen inletts i anställningsförhållande till staten, som i egenskap av arbetsgivare företräds av försvarsministeriet och Försvarsmakten enligt vad som bestäms genom förordning av försvarsministeriet.

*Territorialövervakningslagen*

I en stats suveränitet ingår dess territoriella integritet. Bestämmelser om övervakningen och tryggandet av Finlands territoriella integritet ingår i territorialövervakningslagen (755/2000). Genom territorialövervakningen förebyggs eller uppdagas och klarläggs territorieförseelser och territoriekränkningar. Närmare bestämmelser har med stöd av lagen utfärdats genom statsrådets förordning (971/2000).

Om avvärjande av fientlig verksamhet föreskrivs i 34 § i territorialövervakningslagen. Enligt 2 mom. 4 punkten avses med fientlig verksamhet spaning och elektronisk störning som av en främmande stat orättmätigt riktas mot på finskt territorium belägna objekt som är viktiga med tanke på rikets säkerhet. Enligt 2 mom. 5 punkten är fientlig verksamhet också elektronisk störning som av en främmande stat orättmätigt riktas mot ett finländskt statsluftfartyg eller statsfartyg som utför ett territorialövervakningsuppdrag.

*Lagen om militär disciplin och brottsbekämpning inom försvarsmakten*

Sådant kontraspionage som avses i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014) sker i syfte att förebygga och avslöja brott på finskt territorium. Kontraspionage avser enligt lagen förebyggande och avslöjande av brott som anknyter till olovlig underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret.

Förebyggande och avslöjande av brott definieras i polislagen (872/2011). Genom den brottsbekämpning som Försvarsmakten bedriver förhindras sådan enligt strafflagen (39/1889) kriminaliserad underrättelseverksamhet som en främmande makt riktar mot Finland och som gäller t.ex. Försvarsmaktens prestationsförmåga och sammansättning. Typiska brottsrubriceringar för brott som är föremål för förebyggande och avslöjande är sådana brott som avses i 12 kap. i strafflagen, såsom landsförräderi, spionerі och olovlig underrättelseverksamhet, och högförräderibrott enligt 13 kap. Också mer ordinära brott, såsom egendomsbrott, kan vara föremål för förebyggande och avslöjande av brott, om de ansluter sig till underrättelseverksamhet som riktas mot det militära försvaret eller till verksamhet som äventyrar syftet med det militära försvaret. Exempel på detta är brott mot datasäkerheten eller egendomsbrott som riktar sig mot Försvarsmaktens sekretessbelagda information. Det finns inte någon uttömmande förteckning över brott som berörs av behörigheten.

Försvarsmakten fungerar inom kontraspionaget som specialmyndighet med uppgift att, utan att begränsa Skyddspolisens i lag föreskrivna behörighet, sörja för förebyggande och avslöjande av brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret. Den behörighet Försvarsmakten har att förebygga och avslöja brott är mer begränsad än den som Skyddspolisen har enligt 10 § i polisförvaltningslagen (110/1992) och gäller bara de brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret. På detta område kan behörigheten jämställas med Skyddspolisens allmänna behörighet att förebygga och avslöja brott, men den begränsar inte Skyddspolisens allmänna behörighet. Polisen har enligt lagen övertagningsrätt, alltså rätt att också på eget initiativ ta över ett ärende som omfattas av Försvarsmaktens behörighet att förebygga och avslöja brott.

Vid förebyggande och avslöjande av brott iakttas principerna enligt polislagen också inom Försvarsmakten, och av dem i synnerhet respekten för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna, proportionalitetsprincipen, principen om minsta olägenhet och principen om ändamålsbundenhet.

Skyddspolisen svarar för utredningen av brott som avslöjats på grund av Försvarsmaktens militära kontraspionage.

I fråga om befogenheterna för de tjänstemän som sköter förebyggandet och avslöjandet av brott inom Försvarsmakten gäller enligt lagen om militär disciplin och brottsbekämpning inom försvarsmakten vad som i polislagen föreskrivs om befogenheter vid förebyggande och avslöjande av brott. Tjänstemännen inom försvarsmakten har dock endast vissa av de hemliga metoder för inhämtande av information till sitt förfogande som polisen har till sitt förfogande. Det är fråga om 1) inhämtande av basstationsuppgifter, 2) systematisk observation, 3) förtäckt inhämtande av information, 4) teknisk avlyssning, 5) optisk observation, 6) teknisk spårning och 7) inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning. De enskilda befogenheterna behandlas närmare nedan.

Dessutom avgränsas metoderna för avslöjande av brott genom att det föreskrivs att dessa metoder får användas bara när det är fråga om avslöjande av något av brotten äventyrande av Finlands suveränitet, krigsanstiftan, landsförräderi eller grovt landsförräderi, spioneri eller grovt spioneri, röjande av statshemlighet eller olovlig underrättelseverksamhet. Den tjänsteman som sköter förebyggandet och avslöjandet av brott inom försvarsmakten ska meddela Skyddspolisen om att hemliga metoder för inhämtande av information används.

I lagen om militär disciplin och brottsbekämpning inom försvarsmakten föreskrivs det också om assistans från polisen i sådana fall då den som sköter brottsbekämpning inom Försvarsmakten inte har befogenhet att utföra en åtgärd som behövs för att sköta uppdraget. I praktiken är det fråga om inhämtandet av uppgifter med hjälp av sådana befogenheter som Försvarsmakten inte har. Förebyggandet och avslöjandet av brott utförs av de tjänstemän som är stationerade vid Huvudstaben och Försvarsmaktens underrättelsetjänst, som är underställd Huvudstaben.

Också reservister som deltar i tjänstgöring enligt värnpliktslagen (1438/2007) får vid allvarliga störningar under normalförhållanden samt i undantagsförhållanden användas i uppdrag som anknyter till sådant förebyggande och avslöjande av brott som avses i 102 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Det har ansetts att det är befogat att ge även reservister sådana befogenheter som avses i 86 § i den lagen vid allvarliga stör-

ningar och i undantagsförhållanden, eftersom det kan antas att mängden brott med anknytning till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till verksamhet som äventyrar syftet med det militära försvaret ökar under sådana förhållanden. Det är inte tillåtet att använda personer som fullgör sin värnplikt för sådana uppdrag. Det beror på att deras utbildning fortfarande pågår.

En reservist som har förordnats till en uppgift som gäller förebyggande eller avslöjande av brott enligt lagen om militär disciplin och brottsbekämpning inom försvarsmakten får under ledning och övervakning av en tjänsteman som förordnats att förebygga och avslöja brott inom Försvarsmakten delta i användningen av sådana metoder för informationsinhämtning som avses i 89 § i lagen. Därmed överförs inte någon betydande utövning av offentlig makt på någon annan än en tjänsteman. Reservister omfattas av samma skyldigheter att iaktta sekretess som de som gäller för de tjänstemän som leder och övervakar dem.

Enligt 102 § 2 mom. i lagen om militär disciplin och brottsbekämpning inom försvarsmakten får en reservist som tjänstgör i enlighet med värnpliktslagen och som har förordnats till en uppgift enligt den lagen att förebygga och avslöja brott inom försvarsmakten, delta i utförandet av ett uppdrag enligt 86 § 1 mom. och i användningen av metoderna för inhämtande av information enligt 89 § 1 mom. under ledning och övervakning av en tjänsteman som har förordnats att förebygga och avslöja brott inom Försvarsmakten.

*Polislagen*

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.

Den riksomfattande enhet som svarar för bekämpning av hot mot nationens säkerhet inom polisens organisation är Skyddspolisen. Skyddspolisens viktigaste uppgift är att förebygga och avslöja terrorism, olaglig underrättelseverksamhet, spridning av massförstörelsevapen och brott och förehavanden med kopplingar till extremiströrelser. För att Skyddspolisen ska kunna sköta sin uppgift förutsätts det att den kan inhämta information om sådana brott och förehavanden. Enligt 10 § i polisförvaltningslagen är Skyddspolisens uppgift att under ledning av inrikesministeriet 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. Enligt propositionen med förslag till polisförvaltningslag (RP 155/1991 rd) har man genom skrivningen i bestämmelsen velat rikta uppmärksamheten mot den accentuerade betydelsen av förebyggande verksamhet inom Skyddspolisens uppgiftsområde. Enligt förarbetena till lagen är förebyggandet av gärningar som kan äventyra rikets säkerhet av vital betydelse i Skyddspolisens arbete, medan undersökning av redan inträffade kränkningar av säkerhetsintressen i allmänhet visar på att den förebyggande verksamheten i viss grad har misslyckats.

Bestämmelsen i 10 § i polisförvaltningslagen anger Skyddspolisens verksamhetsområde genom att räkna upp de rättsgoda – inre och yttre säkerhet, stats- och samhällsskicket – som Skyddspolisen har till uppgift att skydda. Några konkreta fenomen och hot mot säkerheten som Skyddspolisen ska bekämpa nämns inte i lagen.

Precis som när det gäller Försvarsmakten krävs det inte någon separat reglering när det gäller inhämtande av information från officiella källor. Eftersom de aktörer som står bakom förehavanden och brott som Skyddspolisen ska bekämpa försöker utföra dem i hemlighet, kan inhämtandet av information i praktiken inte grunda sig på information som är officiellt tillgänglig. Skyddspolisen måste därför fokusera på att inhämta information om verksamhet som sker i hemlighet. För att informationsinhämtningen ska vara effektiv måste den dessutom ske i hemlighet för dem som den riktar sig mot.

Det finns inte några särskilda befogenheter för Skyddspolisen i fråga om inhämtande av information om hot som anknyter till rikets säkerhet. Skyddspolisen är en polismyndighet som i sin verksamhet utövar de befogenheter att inhämta information och andra befogenheter som föreskrivs för polisen.

Skyddspolisens praktiska verksamhet fokuserar på de hemliga metoder för inhämtande av information för att förhindra och avslöja brott som regleras i polislagen. Uppdrag som gäller utredning av brott är för Skyddspolisens del begränsade närmast till utredning av spioneribrott. Skyddspolisen gör sällan förundersökningar.

Enligt 5 kap. 1 § 2 mom. i polislagen avses med förhindrande av brott 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 personens egen verksamhet och tips från en utomstående person och annan indirekt utredning. Till iakttagelser och annan information hör också bl.a. inhämtning av kriminalunderrättelser, observationer, andra tips och slutsatser som grundar sig på brottsanalyser. En förutsättning för användning av en informationsinhämtningsmetod för förhindrande av brott är att det utifrån sådana iakttagelser av en persons verksamhet finns grundad anledning att anta att en person kommer att göra sig skyldig till brott (RP 224/2010 rd, s. 92).

Förhindrande av brott i enlighet med polislagen är förebyggande myndighetsverksamhet i ett tidigt skede. Enligt 5 kap. 1 § 2 mom. avser förhindrande av brott sådana åtgärder som syftar till att förhindra försök till brott och förberedelse till brott. Med förhindrande av förberedelse till brott avses förhindrande av förberedelse till en straffbar handling också när själva förberedelsen inte är kriminaliserad.

Enligt 5 kap. 1 § 3 mom. i polislagen avses med avslöjande av brott 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 på den gråzon som finns mellan förhindrande respektive utredning av brott. Det är inte fråga om utredning av brott, eftersom förutsättningarna för att inleda en förundersökning saknas, och det är inte heller fråga om förhindrande av brott, eftersom det antas att brottet redan har begåtts. Vid avslöjande av brott är det fråga om t.ex. sådana situationer där man fått tips om att ett brott redan har begåtts men det inte finns någon konkret grund för misstanken, dvs. förundersökningslagens tröskel för ”skäl att misstänka” har ännu inte överskridits (RP 224/2010 rd, s. 93).

Bestämmelserna i 5 kap. i polislagen tar upp de hemliga metoder för inhämtande av information som Skyddspolisen får använda 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, styrd användning av informationskällor och kontrollerade leveranser.

Inrikesministeriet fastställer de ärendekategorier som ska undersökas av Skyddspolisen och beslutar vid behov om samarbetet mellan polisenheterna och om fördelningen av undersökningsarrangemangen.

Bland de uppgifter som föreskrivs för Skyddspolisen ingår att aktivt följa utvecklingen i Finlands säkerhetspolitiska omgivning, att proaktivt inhämta information om hot mot säkerheten och att analysera informationen. Analysresultatet produceras i första hand för den högsta statsledningens behov. I 4 a § i polisförvaltningslagen föreskrivs om skyldigheten för Skyddspolisen att underrätta inrikesministern och polisöverdirektören om sådana angelägenheter i skyddspolisens uppgifter som är av samhällelig betydelse. Enligt motiveringen till bestämmelsen ska Skyddspolisen dessutom lämna information direkt till republikens president, statsministern och utrikesministern med beaktande av de utrikes- och säkerhetspolitiska uppgifter som föreskrivits för dem. Skyddspolisen informerar även riksdagens grundlags-, utrikes- och förvaltningsutskott om utvecklingen i säkerhetsläget.

Skyddspolisens viktigaste uppgift är att förebygga och avslöja terrorism, olovlig underrättelseverksamhet, spridning av massförstörelsevapen och brott och förehavanden med kopplingar till extremiströrelser och organiserad brottslighet som äventyrar rikets säkerhet samt i begränsad utsträckning också sköta utredningen av brott med anknytning till sådana fenomen. För att Skyddspolisen ska kunna sköta sin uppgift förutsätts det att den kan inhämta information om sådana brott och förehavanden.

En allmän förutsättning för användning av hemliga metoder för inhämtande av information enligt 5 kap. 2 § 1 mom. i polislagen är att man med en sådan metod kan antas få information som behövs för förhindrande eller avslöjande av brott eller avvärjande av risk för brott. En allmän ytterligare förutsättning för användning av 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 kontrollerade leveranser är enligt 5 kap. 2 § 2 mom. att dessa metoder kan antas vara av synnerlig vikt för förhindrande eller avslöjande av ett brott. För täckoperationer och bevisprovokation genom köp förutsätts dessutom att användningen av metoden är nödvändig för att ett brott ska kunna förhindras eller avslöjas.

När det gäller användningen av olika metoder för informationsinhämtning har det i polislagen föreskrivits om allmänna förutsättningar och särskilda förutsättningar för detta. Särskilda förutsättningar för att använda hemliga metoder för inhämtande av information är framför allt att det är fråga om något av de specificerade brott som varje enskild metod får användas för att förhindra. I de bestämmelser som gäller de enskilda metoderna har man också kunna ställa andra särskilda villkor.

Skyddspolisen kan nästan till alla delar använda sig av samtliga de hemliga metoder för inhämtande av information som ingår i 5 kap. i polislagen för att förhindra sådana terroristbrott som är straffbara enligt 34 a § i strafflagen och sådana brott med anknytning till olovlig underrättelseverksamhet som är straffbara enligt 12 kap. i strafflagen. När det gäller förhindrande av brott som syftar till att sprida massförstörelsevapen och produkter med dubbla användningsområden liksom förhindrande av sådana brott som äventyrar rikets säkerhet som har anknytning till en organiserad kriminell sammanslutning är situationen mer tolkbar.

Befogenheterna har praktiskt betydelse för brottsbekämpningen inom Försvarsmakten i och med 90 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Enligt den kan polisen utföra en sådan enskild åtgärd för Försvarsmaktens räkning som polisen har behörighet till och lämna över de upptagningar och handlingar som erhållits till dem som förebygger och avslöjar brott inom Försvarsmakten, om inte Försvarsmakten har behörighet att utföra åtgärden.

*Lagen om kommunikationsförvaltningen och informationssamhällsbalken*

Enligt 1 § i lagen om kommunikationsförvaltningen (625/2001) finns Kommunikationsverket, som är verksamt inom Kommunikationsministeriets förvaltningsområde, för förvaltningsuppgifter som sammanhänger med kommunikation.

Enligt 2 § 1 mom. har Kommunikationsverket till uppgift att sköta de uppgifter som enligt informationssamhällsbalken ankommer på Kommunikationsverket. Kommunikationsverket har enligt 2 § 2 punkten till uppgift att sköta andra uppgifter som ankommer på Kommunikationsverket enligt andra bestämmelser eller kommunikationsministeriets föreskrifter.

Bestämmelserna i 272 § i informationssamhällsbalken (917/2014) ger teleföretag, sammanslutningsabonnenter och leverantörer av mervärdestjänster samt aktörer som handlar för dessas räkning rätt att analysera innehållet i meddelanden som sänds eller tas emot i deras nät för att bl.a. upptäcka, förhindra och utreda störningar och göra störningarna till föremål för förundersökning.

I de ursprungliga förarbetena till 20 § i lagen om dataskydd vid elektronisk kommunikation (516/2004, RP 125/2003, s. 76) åsyftas med uttrycket ”störningar” bl.a. den omfattande uppsåtliga spridningen och användningen av skadliga program. I detaljmotiveringen till 272 § i informationssamhällsbalken konstateras det att avsikten med bestämmelsen inte är att ändra det rådande rättslaget (RP 221/2013 rd, s. 202).

*Värnpliktslagen*

Enligt 2 § 1 mom. i värnpliktslagen är varje manlig finsk medborgare värnpliktig från ingången av det år när han fyller 18 år till utgången av det år när han fyller 60 år, om inte något annat bestäms i lagen.

Enligt 2 mom. omfattar fullgörandet av värnplikten beväringstjänst, repetitionsövning, extra tjänstgöring och tjänstgöring under mobilisering samt deltagande i uppbåd och besiktning av tjänstedugligheten.

Enligt 3 mom. tjänstgör de värnpliktiga eller hör till reserven eller den ersättande reserven.

I 32 § i lagen föreskrivs om förordnande till repetitionsövningar. Enligt 1 mom. i paragrafen kan en värnpliktig som hör till reserven förordnas till repetitionsövning.

Förordnandet att delta i en repetitionsövning sänds enligt 2 mom. till den värnpliktige minst tre månader innan övningen börjar. Med den värnpliktiges medgivande kan avvikelse från den föreskrivna tiden göras.

När ett tvingande behov som uppstår i Finlands säkerhetspolitiska omgivning förutsätter det, kan värnpliktiga som hör till reserven enligt 3 mom. förordnas till en repetitionsövning som avses i 48 § 4 punkten med avvikelse från den tidsfrist som föreskrivs i 2 mom. Ett förordnande till repetitionsövning ges för varje enskild värnpliktig för högst 30 dagar åt gången.

Enligt 4 mom. fattas beslutet om en sådan repetitionsövning som avses i 3 mom. av republikens president på föredragning av kommendören för försvarsmakten i ett sådant beslutsförfarande som avses i 32 § 2 mom. i lagen om försvarsmakten. Bestämmelser om överföring av ett militärt kommandomål för att avgöras av presidenten i statsrådet finns i 32 § 3 mom. i lagen om försvarsmakten. I 48 § i värnpliktslagen föreskrivs om syftet med repetitionsövningar. Vid reservens repetitionsövningar ska 1) den militära kunskap och förmåga som inhämtats under beväringstjänsten upprätthållas samt utbildning för mera krävande uppgifter ges, 2) de värnpliktiga göras förtrogna med de förändringar som utvecklingen inom det militära försvaret för med sig, 3) trupphelheterna övas i den sammansättning som är planerad för dem eller 4) en flexibel höjning av den militära beredskapen möjliggöras.

Lagen om offentlighet i myndigheternas verksamhet

Enligt 31 § 2 mom. i lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan offentlighetslagen) är den allmänna sekretesstiden för en myndighetshandling 25 år. Försvarsmakten har redan tidigare konstaterat att den allmänna sekretesstiden är för kort i fråga om vissa av Försvarsmaktens lokaler och försvarsmateriel som är i långvarigt bruk, vilket har beaktats i den uppdatering av offentlighetslagen som gjordes 2005 (495/2005). Sekretesstiden kan förlängas med stöd av 31 § i offentlighetslagen, om det skulle vara till skada för landets försvar eller befolkningsskyddet att handlingen blir offentlig. En handling som innehåller sådana uppgifter kan gälla fastigheter, byggnader, konstruktioner, system eller metoder. Möjligheten att förlänga sekretesstiden gäller inte personuppgifter.

Enligt 31 § 4 mom. i offentlighetslagen kan statsrådet förlänga sekretesstiden med högst 30 år. Detta är emellertid avsett att vara en undantagsåtgärd, och det kan inte anses vara ändamålsenligt i sådana fall då det är fråga om regelrätta och förutsägbara behov av sekretess.

2.2.2 Nuläget i fråga om informationsinhämtningen inom Försvarsmakten

*Den militära underrättelseverksamheten som ett led i landets försvar*

Den militära underrättelseverksamheten som Försvarsmakten bedriver i sitt totalförsvarsuppdrag har ansetts grunda sig på Försvarsmaktens lagfästa uppgift att försvara rikets självständighet och territoriella integritet. Den militära underrättelseverksamheten har då ansetts ingå i 2 § 1 mom. 1 punkten underpunkterna a och b i lagen om försvarsmakten, och därmed inte nämnts särskilt i lag.

Den militära underrättelseverksamheten är riktad mot omgivningen utanför Finlands gränser och de hot som kommer därifrån. Den militära underrättelseverksamheten har till uppgift att

forma och upprätthålla en sådan militärstrategisk lägesbild som krävs för det militära beslutsfattandet. För att forma och upprätthålla en sådan lägesbild följer spanings- och övervakningssystemet utvecklingen i Finlands säkerhetspolitiska omgivning, fastställer ändringarna i omgivningen och producerar information om det rådande läget. För att forma den lägesbild som krävs för det militära beslutsfattandet kan det anses att det också behövs information som går att utvinna också på finskt territorium.

Genom den militära underrättelseverksamheten upprätthåller och utvecklar Försvarsmakten försvarsberedskapen. Det viktigaste är att förmågan att få en tidig förvarning om militära hot förbättras för att de beslut landets högsta ledning fattar inför hot som äventyrar staten Finlands suveränitet grundar sig på rättidig lägesinformation och att på så vis göra det möjligt att vidta beredskaps- och motåtgärder vid behov.

Finlands säkerhetspolitiska omgivning är starkt internationaliserad och därmed har information som gäller andra länder ännu större betydelse när det gäller skyddandet av de säkerhetsintressen som Försvarsmakten svarar för. Befogenheterna till militär inhämtning av underrättelser regleras inte i lag. Den militära underrättelseverksamheten inom Försvarsmakten har ordnats med hjälp av Försvarsmaktens interna föreskrifter och anvisningar. Försvarsmakten bedriver sådant samarbete med utländska underrättelsemyndigheter som verksamheten kräver. Syftet med samarbetet är att Försvarsmakten ska få tillgång till sådana utländska underrättelseuppgifter som Försvarsmakten behöver.

De uppgifter som den militära underrättelseverksamheten behöver skaffas genom de metoder olika underrättelseslagen tillämpar och från territorialövervakningssystemet samt från myndigheter och partner genom olika former av samarbete. Uppgifter skaffas också genom internationellt samarbete. I följande avsnitt beskrivs de underrättelsearter som används inom den militära underrättelseverksamheten. Den helhet som den militära underrättelseverksamheten utgör består av inhämtning av underrättelser och kontraunderrättelser och där olika underrättelseslag används för själva verksamheten. För närvarande tillåter lagstiftningen underrättelseinhämtning från öppna källor, radiosignalspaning, inhämtning av bildunderrättelser och personbaserad underrättelseinhämtning inom den inhämtning av information som ansluter sig till det militära försvaret av Finland.

### 2.2.3 Hemliga metoder för inhämtande av information

*Befogenheter inom brottsbekämpningen*

En av de viktigaste uppgifterna inom försvarsmaktens brottsbekämpning är att förebygga och avslöja brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret. Denna uppgift begränsar dock inte Skyddspolisens befogenheter.

Inhämtandet av offentliga uppgifter behöver inte grunda sig på någon särskild i lag föreskriven myndighetsbehörighet. Eftersom de aktörer som står bakom förehavanden och brott som Försvarsmakten ska bekämpa försöker utföra dem i hemlighet, kan inhämtandet av information inte grunda sig på information som är offentligt tillgänglig. Försvarsmakten måste därför fokusera på att inhämta information om verksamhet som sker i hemlighet. För att informationsinhämtningen ska vara effektiv måste den dessutom ske i hemlighet för dem som den riktar sig mot.

Det har inte föreskrivits om några särskilda befogenheter för inhämtandet av information som ansluter sig till hot mot rikets säkerhet, utan den har delvis ansetts grunda sig på Försvarsmaktens uppgifter enligt 2 § i lagen om försvarsmakten.

Försvarsmakten kan vid brottsbekämpningen använda sig av vissa av de befogenheter som föreskrivs för polisen. Enligt 89 § 1 mom. i lagen om militär disciplin och brottsbekämpning inom försvarsmakten gäller i fråga om befogenheterna för de tjänstemän som sköter förebyggandet och avslöjandet av brott inom försvarsmakten vad som i polislagen föreskrivs om befogenheter vid förebyggande och avslöjande av brott. Av de metoder för hemligt inhämtande av information som avses i 5 kap. i polislagen har de tjänstemän som sköter förebyggandet och avslöjandet av brott inom försvarsmakten dock till sitt förfogande endast 1) inhämtande av basstationsuppgifter, 2) systematisk observation, 3) förtäckt inhämtande av information, 4) teknisk avlyssning, 5) optisk observation, 6) teknisk spårning, 7) inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning. Av de övriga hemliga metoder för inhämtande av information som avses i 5 kap. i polislagen har tjänstemännen inte till sitt förfogande teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teleövervakning med samtycke av den som innehar teleadress eller teleterminalutrustning, förtäckt inhämtande av information, teknisk observation av utrustning, täckoperation, bevisprovokation genom köp, användning av informationskällor, styrd användning av informationskällor och kontrollerade leveranser.

Även om det föreskrivs om hemliga metoder för inhämtande av information i polislagen, föreskrivs det särskilt om utövandet av befogenheterna inom Försvarsmakten i 87 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Enligt bestämmelsen utövas de befogenheter som har föreskrivits för en polisman som hör till befälet och för en anhållningsberättigad polisman av den officer som förordnats till uppgiften som den biträdande avdelningschef som svarar för kontraspionage vid huvudstaben samt en militärjurist. De befogenheter som har föreskrivits för en polisman utövas av en officer, specialofficer, institutsofficer eller underofficer som har förordnats till uppdraget att förebygga och avslöja brott eller en annan tjänsteman som är anställd vid Försvarsmakten och har förordnats till uppdraget.

*Samverkan med polisen vid hemligt inhämtande av information.*

Enligt 90 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten kan polisen på en skriftlig begäran av en tjänsteman som sköter brottsbekämpning utföra en sådan enskild åtgärd som polisen har behörighet till, om de som förebygger och avslöjar brott inom försvarsmakten inte har behörighet att utföra en enskild åtgärd som behövs för att sköta ett uppdrag.

Enligt 2 mom. i paragrafen lämnar polisen över de upptagningar och handlingar som erhållits genom en åtgärd som avses i 1 mom. till dem som förebygger och avslöjar brott inom försvarsmakten. Polisen får lämna över upptagningarna och handlingarna obehandlade. De som förebygger och avslöjar brott inom försvarsmakten svarar då för att upptagningarna och handlingarna granskas samt för andra uppgifter med anknytning till behandlingen av informationen på det sätt som föreskrivs i 5 kap. i polislagen.

Enligt 3 mom. utförs ett uppdrag som gäller förebyggande och avslöjande av brott i samverkan med polisen när sakens natur kräver det. Den som förebygger och avslöjar brott inom försvarsmakten och polismyndigheten kommer överens om de frågor som sammanhänger med uppdraget. Polisen har också rätt att av ett särskilt skäl på eget initiativ överta ett ärende som gäller förebyggande och avslöjande av brott för att undersöka det.

2.2.4 Allmänt om hemliga metoder för inhämtande av information

Såsom framgår av det som sägs ovan grundar sig Försvarsmaktens hemliga metoder för inhämtande av information på polislagen. De allmänna förutsättningarna och metoderna för hemlig inhämtande av information kan inte granskas utan att samtidigt granska bestämmelserna i polislagen vid sidan av bestämmelserna i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Förutsättningarna för användningen av hemliga metoder för inhämtande av information skiljer sig åt inom Försvarsmakten och polisen, även om själva det hemliga inhämtandet av information sker på samma sätt.

*Allmänna förutsättningar för användning av hemliga metoder för inhämtande av information*

Enligt 5 kap. 1 § 2 mom. i polislagen avses med förhindrande av brott 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 personens egen verksamhet och tips från en utomstående person och annan indirekt utredning. Till iakttagelser och annan information hör också bl.a. inhämtning av kriminalunderrättelser, observationer, andra tips och slutsatser som grundar sig på brottsanalyser. En förutsättning för användning av en informationsinhämtningsmetod för förhindrande av brott är att det utifrån sådana iakttagelser av en persons verksamhet finns grundad anledning att anta att en person kommer att göra sig skyldig till brott (RP 224/2010 rd, s. 92).

Enligt 5 kap. 1 § 3 mom. i polislagen avses med avslöjande av brott 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 på den gråzon som finns mellan förhindrande respektive utredning av brott. Det är inte fråga om utredning av brott, eftersom förutsättningarna för att inleda en förundersökning saknas, och det är inte heller fråga om förhindrande av brott, eftersom det antas att brottet redan har begåtts.

De hemliga metoder för inhämtande av information som myndigheterna har till sitt förfogande kan indelas i olika grupper utifrån användningssätt och användningsändamål. De tekniska metoder som får användas för att inhämta information om ett övervakningsobjekts kommunikation är teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teleövervakning med samtycke av den som innehar teleadress eller teleterminalutrustning och teknisk avlyssning. Som traditionella metoder för inhämtande av personuppgifter betraktas användning av informationskällor och därmed förknippad styrd användning av informationskällor. När informationskällor används skaffas information om objektet via en mellanhand. När kommunikationen mellan den som inhämtar information och antingen den som fungerar som mellanhand eller objektet självt omfattar skenmanövrar är de metoder som används för inhämtande av personuppgifter förtäckt inhämtande av information, täckoperation och bevisprovokation genom köp. Metoderna för teknisk observation av objektets uppförande är teknisk avlyssning, optisk övervakning, teknisk spårning och teknisk observation av utrustning. Systematisk observation i sin tur grundar sig på hur objektet uppför sig vid observation som baserar sig på sinnesförnimmelser.

En allmän förutsättning för användning av hemliga metoder för inhämtande av information enligt 5 kap. 2 § 1 mom. i polislagen är att man med en sådan metod kan antas få information som behövs för förhindrande eller avslöjande av brott eller avvärjande av risk för brott. En allmän ytterligare förutsättning för användning av 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 kontrollerade leveranser är enligt 5 kap. 2 § 2 mom. att dessa metoder kan antas vara av synnerlig vikt för förhindrande eller avslöjande av ett brott. För täckoperationer och bevisprovokation genom köp förutsätts dessutom att användningen av metoden är nödvändig för att ett brott ska kunna förhindras eller avslöjas.

Genom de hänvisningar till polislagen som finns i lagen om militär disciplin och brottsbekämpning inom försvarsmakten har det föreskrivits om allmänna förutsättningar och särskilda förutsättningar för användningen av olika metoder för informationsinhämtning. Särskilda förutsättningar för att använda hemliga metoder för inhämtande av information är framför allt att det är fråga om något av de specificerade brott som varje enskild metod får användas för att förhindra. I de bestämmelser som gäller de enskilda metoderna har man också kunna ställa andra särskilda villkor.

Sådana hemliga metoder för avslöjande av brott som nämns ovan får användas bara om det är fråga om brott som rubriceras som landsförräderi eller terrorism.

Ett gemensamt drag hos de hemliga metoder för inhämtande av information som försvarsmakten använder är att de utgår från person och brottstyp. De kan bara riktas mot en verksamhet eller användas för att inhämta information om sådan verksamhet som bedrivs av en person i en situation där det finns grundad anledning att anta att personen i fråga i framtiden kommer att göra sig skyldig till ett brott av en viss allvarlighetgrad eller där personen redan har gjort sig skyldig till ett visst brott eller till förberedelse för ett sådant brott. Om en sådan brottsbekämpningsgrund som hänför sig till en viss person saknas, kan en sådan metod för hemligt inhämtande av information som avses i polislagen inte användas. Inhämtandet av annan underrättelseinformation måste således baseras på öppna källor och på sådan information som försvarsmakten via sitt samarbetsnätverk får av andra myndigheter eller av privata aktörer.

*Metoder för inhämtande av uppgifter som baserar sig på telekommunikation*

Metoder för inhämtande av uppgifter som baserar sig på telekommunikation är teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, teleövervakning med samtycke av den som innehar teleadress eller teleterminalutrustning och inhämtande av basstationsuppgifter Av dessa metoder får Försvarsmakten inom brottsbekämpningen använda sig av inhämtande av basstationsuppgifter.

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 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. Eftersom denna person uttryckligen måste nämnas i begäran om och tillståndet till teleavlyssning, kan teleavlyssningen inte riktas mot någon annan person. I 2 mom. nämns det vilka brott polisen får använda sig av teleavlyssning för att förhindra.

Det föreskrivs uttryckligen i 5 kap. 5 § 1 mom. att teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en viss person. Lagen tillåter också avlyssning av okända personers meddelanden, om de mottas eller skickas till en person som med fog kan antas göra sig skyldig till de brott som avses ovan. Enligt 2 mom. kan polisen för att förhindra brott 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 att personen har en koppling till en teleadress eller teleterminalutrustning, eller till en teleadress eller teleterminalutrustning som personen använder eller antas använda. Beviströskeln är inte hög i detta avseende. I praktiken måste det skaffas ett nytt domstolstillstånd för varje ny teleadress eller teleterminalutrustning som personen använder eller antas använda. Polisen kan enligt 3 mom. dessutom beviljas tillstånd till teleavlyssning, om det är nödvändigt för att avvärja en allvarlig fara som omedelbart hotar liv eller hälsa.

Om inhämtande av information i stället för teleavlyssning föreskrivs i 5 kap. 6 § i polislagen. Bestämmelserna om teleavlyssningen gällde ursprungligen telefonnätet. När de gällande bestämmelserna om teleavlyssning tillkom åtgärdades vissa av de brister i bestämmelserna som kopplingen till en viss sorts teknik innebar. Enligt 1 mom. kan polisen för att förhindra brott, om det är sannolikt att ett meddelande som avses i 5 § och dess identifieringsuppgifter inte längre är tillgängliga genom teleavlyssning, beviljas tillstånd att inhämta informationen hos ett teleföretag eller en sammanslutningsabonnent, under de förutsättningar som anges i 5 §. Det är fråga om ett beslag som omfattas av förutsättningarna för teleavlyssning, om åtgärden riktas mot ett teleföretag eller en sammanslutningsabonnent. Inhämtande av information i stället för teleavlyssning lämpar sig t.ex. på sådana situationer där det meddelande som inhämtas med hjälp av teleavlyssning har försvunnit eller förstörts, men det fortfarande tekniskt finns att tillgå hos teleföretaget eller sammanslutningsabonnenten. Syftet med regleringen har varit att förhindra att villkoren för att använda sig av teleavlyssning kringgås genom att data konfiskeras på vägen till teleföretaget eller sammanslutningsabonnenten.

Enligt 5 kap. 6 § 2 mom. kan polisen, 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, för att förhindra brott beviljas tillstånd till inhämtande av information i stället för teleavlyssning, om de förutsättningar som anges i 5 § finns. Utan denna bestämmelse kunde information inhämtas t.ex. som teknisk avlyssning, eftersom ett meddelande som passerat teleadressens gränssnitt och överförts till detta slag av personlig anordning inte längre omfattas av teleavlyssningsbefogenheten. Sådana personliga tekniska anordningar som avses i momentet är t.ex. bluetooth-hörlurar. Avlyssning av ett samtal via högtalarfunktion eller ett i övrigt högljutt samtal är inte sådant inhämtande av information i stället för teleavlyssning som avses i momentet.

I 5 kap. i polislagen regleras de förbud som avser avlyssning och observation i dess 50 §. 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 § i tvångsmedelslagen får teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation inte riktas mot meddelanden mellan följande parter: 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. I 3 mom. till paragrafen anges att åtgärden ska avbrytas och de upptagningar som fåtts genom den och anteckningarna om de uppgifter som fåtts genom den genast ska utplånas, om det under teleavlyssningen, inhämtandet av information i stället för teleavlyssning, den tekniska avlyssningen eller den optiska observationen eller vid något annat tillfälle framkommer att det är fråga om ett meddelande som inte får avlyssnas eller observeras. 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.

Enligt 5 kap. 7 § 1 mom. i polislagen beslutar domstolen 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). Tillstånd till teleavlyssning och till inhämtande av sådan information som avses i 6 § 2 mom. kan enligt 7 § 2 mom. ges för högst en månad åt gången.

I yrkandet och beslutet ska mycket detaljerade uppgifter anges. Vid översynen av polislagen och tvångsmedelslagen (RP 224/2010 rd och RP 222/2010 rd) framhölls skyldigheten att framlägga och motivera de fakta utifrån vilka domstolen kan dra sina egna slutsatser om huruvida förutsättningarna för att använda hemliga metoder för inhämtande av information är uppfyllda. Det är framför allt fråga om de allmänna förutsättningar som redovisats ovan och om de uttryckliga förutsättningar som anges i 5 kap. 5 och 6 § i polislagen.

Enligt 5 kap. 8 § 1 mom. i polislagen 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. Identifieringsuppgifter är enligt 2 § 8 punkten i lagen om dataskydd vid elektronisk kommunikation sådana uppgifter om ett meddelande som kan förknippas med en abonnent eller användare och behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. I gällande bestämmelser används en definition av identifieringsuppgifter som grundar sig på definitionen i 2 § 8 punkten i lagen om dataskydd vid elektronisk kommunikation. Det är inte möjligt att definiera identifieringsuppgifter på ett uttömmande och entydigt sätt. Begränsningen av definitionen till att gälla uppgifter om ett meddelande innebär trots det att sådan styrningstrafik mellan datorer som inte har samband med ett meddelande inte omfattas av skyddet för konfidentiell kommunikation. Enligt 5 kap. 8 § 2 mom. i polislagen kan polisen för att förhindra brott beviljas tillstånd till teleövervakning av en teleadress eller teleterminalutrustning som innehas eller sannolikt annars används av 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 momentet.

I 5 kap. 9 § i polislagen ingår bestämmelser om teleövervakning som baserar sig på samtycke. Enligt paragrafen får polisen, med samtycke av den som innehar en teleadress eller teleterminalutrustning, för att förhindra brott rikta teleövervakning mot adressen eller utrustningen, om någon på grund av sina yttranden eller sitt uppträdande i övrigt med fog kan antas göra sig skyldig till ett brott som nämns i bestämmelsen. Att teleadressen eller teleterminalutrustningen

ska innehas av den som ger sitt samtycke innebär här ett faktiskt innehav. Sålunda kan t.ex. en arbetsgivare inte ge sitt samtycke till teleövervakning av en mobiltelefon som används av en arbetstagare.

Enligt 5 kap. 10 § i polislagen ska domstolen besluta om teleövervakning för att förhindra eller avslöja brott och om sådan teleövervakning som grundar sig på innehavarens samtycke som avses i 9 § på yrkande av en anhållningsberättigad tjänsteman. Tillstånd kan beviljas för högst en månad åt gången. Tillstånd kan beviljas så att det gäller även en viss tid före beslutet som 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. Inhämtande av basstationsuppgifter kan därmed gälla även teleadresser och teleterminalutrustningar som registreras i framtiden. I paragrafens 2 mom. föreskrivs om förutsättningarna för inhämtande av basstationsuppgifter. Med stöd av bestämmelsen i momentet kan polisen beviljas tillstånd att inhämta basstationsuppgifter från en basstation i närheten av den förmodade vistelseorten vid den förmodade brottstidpunkten för en person som på grund av sina yttranden eller hotelser, sitt uppträdande eller i övrigt med fog kan antas göra sig skyldig till brott enligt förutsättningarna för teleövervakning i 8 § 2 punkten om.

I 5 kap. 12 § i polislagen föreskrivs om förfarandet för beslut om inhämtande av basstationsuppgifter. Enligt 1 mom. fattar domstolen beslut om inhämtande av basstationsuppgifter 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 även omfatta uppgifter som föregått tidpunkten för beslutet, eftersom sådana uppgifter kan vara relevanta för förhindrande av brott. Det väsentliga är att informationens relevans kan motiveras. Enligt lagen om militär disciplin och brottsbekämpning inom försvarsmakten fattas beslut i brådskande situationer av den officer vid Försvarsmakten som förordnats till uppgiften som den biträdande avdelningschef som svarar för kontraspionage vid huvudstaben samt en militärjurist.

*Olika metoder för observation*

Till metoderna för observation hör 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 en teleadress eller teleterminalutrustning samt installation och avinstallation av utrustning, metoder eller programvara som stöder dessa metoder. Försvarsmakten får använda samtliga dessa metoder för observation i sin brottsbekämpning.

I 5 kap. 13 § i polislagen finns bestämmelser om systematisk observation. I 1 mom. ingår en allmän definition. Enligt den avses med observation iakttagande av en viss person i hemlighet i syfte att inhämta information. Enligt 2 mom. i den föreslagna paragrafen avses med systematisk observation annan än kortvarig observation av en person som med fog kan antas göra sig skyldig till ett brott. I enlighet med definitionen för observation sker även systematisk observation i hemlighet, vilket även innefattar att interaktion med personen undviks. Enligt 3 mom. får polisen för att förhindra brott 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 före-

skrivna strängaste straffet är fängelse i minst två år eller till stöld eller häleribrott. Det anges i 4 mom. att observation enligt paragrafen inte får riktas mot utrymmen som används för stadigvarande boende. Observation med hjälp av sinnesförnimmelser får trots det riktas mot en person som omfattas av hemfridsskyddet för att förhindra eller avslöja brott.

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

Enligt 5 kap. 15 § 1 mom. i polislagen avses med förtäckt inhämtande av information inhämtande av information genom kortvarig interaktion med en viss person där falska, vilseledande eller förtäckta uppgifter används för att hemlighålla polismannens uppdrag. Det som är betecknande för förtäckt inhämtande av information i jämförelse med utövandet av befogenheterna för observation och systematisk observation är uttryckligen en strävan efter personlig kontakt eller motsvarande interaktion med den som är föremål för inhämtande av information. Det som skiljer förtäckt inhämtande av information från en täckoperation är att det i detta fall inte är fråga om infiltration i syfte att skapa ett långvarigt förtroendeförhållande. Vid förtäckt inhämtande av information är det möjligt att använda falsk, vilseledande är förtäckt information för att undvika att bli avslöjad. Enligt 2 mom. får polisen använda förtäckt inhämtande av information, om det på grund av en persons yttranden eller uppträdande i övrigt med fog finns anledning att anta att denne kommer att göra sig skyldig till ett brott som nämns i momentet. Förtäckt inhämtande av information får emellertid också rikta sig mot andra personer än den som med fog kan antas göra sig skyldig till ett brott.

Enligt 5 kap. 16 § 1 mom. ska chefen för centralkriminalpolisen, chefen för skyddspolisen, chefen för polisinrättningen eller en för uppdraget förordnad anhållningsberättigad polisman som särskilt utbildats för hemligt inhämtande av information besluta om förtäckt inhämtande av information. I 2 mom. föreskrivs det om innehållet i ett beslut om förtäckt inhämtande av information. Beslutet ska fattas skriftligen. När det gäller utövandet av befogenheten förutsätts det att den polisman som ansvarar för uppdraget utnämns särskilt och att denne bl.a. ska se till att det i praktiken inte handlar om en täckoperation. Enligt 3 mom. ska beslutet vid behov ses över när omständigheterna förändras. Momentet förpliktar den ansvariga polismannen att övervaka att det fortfarande finns förutsättningar för förtäckt inhämtande av information. Förtäckt inhämtande av information får inte genomföras i en bostad ens om bostadens innehavare har gett sitt medgivande till att någon går in i bostaden. Som förtäckt inhämtande av information i bostaden anses dock inte att en polisman som uppträder som bud begär kvittering på en försändelse av mottagaren till försändelsen i exempelvis bostadens tambur.

Enligt 5 kap. 17 § 1 mom. i polislagen avses med teknisk avlyssning 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. Tangentbordsavlyssning som genomförs med hjälp av programvara eller en anordning via ett datasystem omfattas också av definitionen. Skillnaden mellan teknisk avlyssning och den tekniska observation av utrustning som avses i 5 kap. 23 § i polislagen är den att polisen genom teknisk observation av utrustning kan inhämta annan information som lagrats i eller processeras av anordningen än sådan som gäller kommunikation. Det anges i 2 mom. att optisk observation inte får riktas mot utrymmen som används för stadigvarande boende. Enligt 3 mom. får polisen i syfte att förhindra brott rikta teknisk avlyssning mot en person som befinner sig i ett utrymme eller på en plats utanför det

utrymme som används för stadigvarande boende och där det kan tänkas att personen sannolikt befinner sig eller som denne besöker. Teknisk avlyssning kan med stöd av momentet 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 ett brott som nämns i momentet. Ytterligare en förutsättning för användning av teknisk avlyssning är enligt 5 kap. 2 § 2 mom. att metoden bara får användas om den kan antas vara av synnerlig vikt för förhindrande eller avslöjande av ett brott. Enligt 5 kap. 17 § 5 mom. har polisen trots 2 mom. 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 (s.k. stormningsavlyssning). I fråga om granskning av undersökning av upptagningar som uppkommit vid teknisk avlyssning och om avbrytande av teknisk avlyssning föreskrivs det närmare i 5 kap. 51, 52 och 56 §. Också i dessa fall kan bestämmelserna om överskottsinformation i 5 kap. 53–55 § polislagen bli tilllämpliga. När det gäller teknisk avlyssning är det skäl att nämna att teleavlyssning och teleövervakning är planerade för telefonnätet, medan sådant inhämtande av information som är riktat mot hemlig kommunikation som försiggår i datanät delvis måste ske med stöd av befogenheter av observationstyp, närmare bestämt just 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. Enligt 2 mom. ska beslut om teknisk avlyssning som avses i 17 § 5 mom. och om annan än i 1 mom. avsedd teknisk avlyssning fattas av en anhållningsberättigad polisman. Enligt 3 mom. kan tillstånd till teknisk avlyssning ges och beslut om sådan fattas för högst sex månader åt gången. I 4 mom. föreskrivs det om vad yrkandet och beslutet ska innehålla. En särskild resultatförväntan är förknippad med teknisk avlyssning. Därför måste det i yrkandet och beslutet framföras vilka omständigheter som ligger till grund för ett antagande om att ett visst utrymme eller en viss plats är en sådan där den person som är föremål för informationsinhämtningen sannolikt kommer att vistas eller besöka. Om teknisk avlyssning riktas mot ett utrymme behöver det trots det inte specificeras med samma noggrannhet som när det gäller den misstänktes bostad, om det inte vid tidpunkten för beslutet är säkert vilket utrymme det är fråga om.

Med optisk observation avses enligt 5 kap 19 § 1 mom. 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. Precis som när det gäller teknisk avlyssning kan optisk observation utöver mot ett utrymme eller en plats också rikta sig mot en viss person. Optisk observation skiljer sig från observation och systematisk observation i det avseendet att man vid optisk observation använder utplacerade tekniska anordningar, metoder eller programvaror. Det anges i 2 mom. att optisk observation inte får riktas mot utrymmen som används för stadigvarande boende. Förbudet mot optisk observation i en bostad gäller emellertid inte om det är fråga om att förhindra eller avslöja brott med hjälp av optisk observation vid en stormning. Enligt 3 mom. har polisen rätt att rikta optisk observation mot personer utanför utrymmen som används för stadigvarande boende för att förhindra brott. 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 för-

utsättning 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., alltså brott som utgör 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 är 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.

Beslut om optisk observation ska enligt 5 kap. 20 § 1 mom. i polislagen 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 optisk observation 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 fattas för högst sex månader åt gången. I 4 mom. föreskrivs det om vad yrkandet och beslutet om optisk observation ska innehålla.

Enligt definitionen i 5 kap. 21 § 1 mom. i polislagen 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. ingår bestämmelser 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 denne 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. i sådana fall då också teknisk avlyssning vore möjlig. Enligt 4 mom. har polisen dessutom alltid 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 den persons liv eller hälsa som ska gripas eller skyddas (observation inför en stormning).

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 beslut om teknisk spårning som avses i 21 § 4 mom. (observation inför en stormning) och om annan än i 1 mom. avsedd teknisk spårning fattas av en anhållningsberättigad polisman. Enligt 3 mom. kan tillstånd ges och beslut fattas för högst sex månader åt gången. I 4 mom. föreskrivs det om vad yrkandet och beslutet om teknisk spårning ska innehålla.

Bestämmelsen i 5 kap. 23 § 1 mom. innehåller en definition av teknisk observation av utrustning. Det är fråga om 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. Med hjälp av teknisk observation av utrustning kan en teknisk anordning och allmänt taget den information som den misstänkta personen har sparat och som den tekniska anordningen innehåller observeras. Sådan information kan finnas i dokument som har sparats i den tekniska anordningen. Genom teknisk observation av utrustning kan interaktionen mellan personen i fråga och den tekniska anordningen följas. I 2 mom. föreskrivs om gränsdragningen för detta teletvångsmedel. Enligt bestämmelsen får information om innehållet i ett meddelande eller om identifieringsuppgifter som avses i 8 § inte inhämtas genom teknisk observation av utrustning. Polisen får rikta teknisk observation av utrustning mot en dator eller en liknande teknisk anordning som personen i fråga sannolikt använder, eller mot dess programvara. Ytterligare en förutsättning för användning av teknisk observation av utrustning är enligt 2 § 2 mom. att metoden bara får användas om den kan antas vara av synnerlig vikt för förhindrande eller avslöjande av ett brott. Teknisk observation av utrustning kan användas för s.k. tangentbordsavlyssning bara i den mån den som använder anordningen inte skriver något meddelande. För genomförande av tangentbordsavlyssning får polisen använda sig av befogenheten för teknisk avlyssning enligt 17 §. Grundbrotten för denna befogenhet är desamma som för teknisk observation av utrustning. Enligt 23 § 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 paragrafens 2 mom. kan tillstånd beviljas för högst en månad åt gången. I 3 mom. föreskrivs det om vad yrkandet och beslutet om teknisk observation av utrustning ska innehålla.

Enligt 5 kap. 25 § 1 mom. i polislagen får polisen för att förhindra brott med hjälp av 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. Enligt 2 mom. får polisen för inhämtande av de uppgifter som avses i 1 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 detta moment och att de inte på grund av sina egenskaper orsakar skadliga störningar i ett allmänt kommunikationsnäts anordningar eller tjänster. Enligt 3 mom. får beslut om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning fattas av en anhållningsberättigad polisman. Enligt lagen om militär disciplin och brottsbekämpning inom försvarsmakten fattas beslut om användningen av en metod för inhämtande av information av den officer som förordnats till uppgiften som den biträdande avdelningschef som svarar för kontraspionage vid huvudstaben samt en militärjurist.

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. Det föreskrivs i 2 mom. att anord-

ningar, metoder och programvara som används för teknisk observation får 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. Anordningar, metoder och programvara som används för teknisk observation får installeras i utrymmen som används för stadigvarande boende utan tillstånd av domstol endast för att avvärja sådan fara som anges i momentet, dvs. när de används för observation inför en stormning.

*Täckoperationer och bevisprovokation genom köp*

Täckoperationer och bevisprovokation genom köp anses vara de hårdaste metoderna för hemligt inhämtande av information, eftersom villkoren för att få använda dem är synnerligen strikta. Försvarsmakten har inte några lagfästa befogenheter att använda täckoperationer eller bevisprovokation genom köp i sin brottsbekämpning.

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. Polisen får enligt 2 mom. rikta en täckoperation mot en person som på grund av sina yttranden eller sitt uppträdande i övrigt med fog kan antas komma att göra sig skyldig eller medverka till något annat i 10 kap. 3 § i tvångsmedelslagen avsett brott än grovt ordnande av olaglig inresa eller grovt tullredovisningsbrott, eller som med fog kan antas komma att göra sig skyldig eller medverka till ett brott som avses i 17 kap. 18 § 1 mom. 1 punkten i strafflagen. En förutsättning är dessutom att inhämtandet av information måste anses 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 nätbaserade täckoperationer. Enligt momentet får polisen rikta en datanätsbaserad täckoperation mot en person, om det med fog kan antas att personen kommer att göra sig skyldig till ett 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 en täckoperation. Därför får en täckoperation företas 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 föreskrivs om brottsförbud och i 30 § om deltagande i en organiserad kriminell sammanslutning och i kontrollerade leveranser. I 31 och 32 § föreskrivs om framställning om och plan för en täckoperation respektive beslut om en täckoperation. Om beslut om förutsättningarna för täckoperation och om utvidgad täckoperation föreskrivs i 33 och 34 §.

Enligt 5 kap. 35 § 1 mom. i polislagen avses med bevisprovokation genom köp 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 hand 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 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.

Den som genomför bevisprovokation genom köp får enligt 3 mom. utföra bara sådant inhämtande av information som är nödvändigt för genomförandet av 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 denne inte annars skulle begå. Bestämmelserna om husrannsakan får inte heller kringgås vid bevisprovokation genom köp. Bevisprovokation genom köp får därför enligt 4 mom. företas 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 bevisprovokation genom köp och om beslut och planer som gäller genomförande av bevisprovokation genom köp ingår i 5 kap. 36–38 § i polislagen.

Om säkerheten för en polisman vid förtäckt inhämtande av information, en täckoperation och vid bevisprovokation genom köp föreskrivs i 5 kap. 39 § i polislagen. En anhållningsberättigad polisman får enligt 1 mom. 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. Enligt 2 mom. får avlyssningen och observationen 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.

*Styrd användning av informationskällor och kontrollerade leveranser*

Bestämmelser om användning av informationskällor och om kontrollerade leveranser ingår i 5 kap. 40–43 § i polislagen. Försvarsmakten har inte några lagfästa befogenheter att använda styrd användning av informationskällor eller kontrollerade leveranser i sin brottsbekämpning.

Enligt 5 kap. 40 § 1 mom. i polislagen avses med användning av informationskällor annat än sporadiskt konfidentiellt mottagande av information av betydelse för utredning av brott 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). Enligt 3 mom. får en informationskälla inte vid styrd användning av informationskällor ombes 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 informationskällan 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 informationsinhämtningen. Om beslut om styrd användning av informationskällor föreskrivs i 5 kap. 42 § i polislagen.

Om kontrollerade leveranser och förutsättningar för sådana föreskrivs i 5 kap. 43 § i polislagen. Enligt 1 mom. i paragrafen 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. 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. Bestämmelser om beslut om kontrollerade leveranser ingår i 5 kap. 44 §.

2.2.5 Försvarsmaktens andra metoder för inhämtande av information

Försvarsmakten kan för utförande av sina lagstadgade uppgifter även utöva andra än de lagstadgade befogenheterna. Sådana är underrättelseinhämtning ur öppna källor, personbaserad underrättelseinhämtning i internationell verksamhet, bildunderrättelser, geografisk underrättelseinhämtning och radiosignalspaning.

*Underrättelseinhämtning ur öppna källor*

Underrättelser ur öppna källor (open source intelligence, OSINT) är kunskap som baserar sig på information som inhämtats från öppna källor och som har uppdelats, värderats och filtrerats på ett enhetligt sätt.

Information från öppna källor består av uppgifter som varje medborgare lagligt har tillgång till på begäran eller genom att själv göra observationer. Typiska informationskällor är litteratur, statistik, kartor, tidningar, publikationer, televisions- och radiosändningar riktade till allmänheten samt innehållet på sociala medier. Informationsinhämtning ur öppna källor kan delas upp i informationsinhämtning som baserar sig på avgränsade underrättelsefrågor och i medieövervakning, som har som syfte att stödja skapandet av en lägesbild för underrättelseinhämtningen.

Vid underrättelseinhämtning ur öppna källor är informationsinhämtningen huvudsakligen inriktad på mer omfattande fenomen eller händelser. Vid långvarig informationsinhämtning är dock t.ex. övervakning av enskilda användarkonton i sociala medier viktigt för att förstå en händelse eller för att bedöma en uppgifts tillförlitlighet.

I underrättelseinhämtning ur öppna källor anses inte ingå aktivt deltagande i t.ex. diskussioner som förs på Internet i syfte att inhämta information. Information kan i enlighet med andra myndigheter inhämtas också genom att köpa eller med hjälp av tredje parter (t.ex. experter, mediebevakningsföretag).

Underrättelseinhämtning ur öppna källor används som stöd för annan form av underrättelseinhämtning eller som självständig form av underrättelseinhämtning där andra former av underrättelseinhämtning inte är möjliga eller effektiva. Kännetecknande för denna form av underrättelseinhämtning är den stora mängden information och möjligheten till desinformation. Under de senaste åren har i synnerhet antalet observationer via sociala medier ökat i förhållande till andra källor.

Till fördelarna med underrättelseinhämtning ur öppna källor hör att den är snabb, fördelaktig, geografiskt obegränsad och att information kan insamlas om kommande händelser. En underrättelseprodukt som enbart baserar sig på öppna källor är ofta till sin skyddsnivå mer offentlig än andra underrättelseprodukter, varvid produkten är mer användbar.

*Bildunderrättelser*

Med hjälp av bildunderrättelser (Imagery intelligence, IMINT) produceras det med elektrooptiska metoder och radarbilder analyserad information och en hotbild vad gäller militära mål och mål som hänför sig till militär verksamhet samt verksamheten på dessa.

*Geografisk underrättelseinhämtning*

Med geografisk underrättelseinhämtning avses informationsinhämtning om främmande staters geografiska förhållanden och verksamhetsmiljön i området. Syftet med geografisk underrättelseinhämtning är att beskriva, bedöma och presentera vissa objekt, områden, naturfenomen och förhållanden. Vid geografisk underrättelseinhämtning utnyttjas t.ex. nationellt och internationellt geografiskt informationsmaterial och bildmaterial, uppgifter om förhållanden samt statistiska uppgifter. Militärunderrättelsemyndigheten kan även av utomstående aktörer beställa sådan information till stöd för sin egen underrättelseinhämtning.

*Personbaserad underrättelseinhämtning i internationell verksamhet*

Personbaserad underrättelseinhämtning (Human intelligence, HUMINT) är i allmänhet en form av underrättelseinhämtning som har som syfte att med hjälp av utbildad personal inhämta information när informationsinhämtningen inriktas på personer samt handlingar och elektroniska upptagningar som är i deras besittning.

I nuläget kan personbaserad underrättelseinhämtning användas i begränsad omfattning vid brottsbekämpning inom Försvarsmakten, men personbaserad underrättelseinhämtning kan även genomföras inom Försvarsmaktens internationella verksamhet.

Försvarsmakten har vid informationsinhämtning till sitt förfogande det nätverk av militärattachéer som tjänstgör vid Finlands beskickningar i utlandet. Enligt artikel 3 i Wienkonventionen om diplomatiska förbindelser omfattar en diplomatisk beskicknings uppgifter bl.a. att med alla lagliga medel hålla sig underrättad om förhållandena och utvecklingen i den mottagande staten samt att avge rapporter därom till den sändande statens regering. I artikel 7 i konventionen nämns av beskickningspersonalen särskilt militär-, marin- och flygattachéer. I de lagar som gäller Försvarsmakten finns inga bestämmelser om befogenheterna för de tjänstemän vid Försvarsmakten som tjänstgör vid beskickningar. I vid bemärkelse kan Finlands nätverk av försvarsattachéer anses höra till området för personbaserad underrättelseinhämtning.

Personbaserad underrättelseinhämtning kan också användas i vissa situationer vid krishanteringsinsatser. Vid krishanteringsinsatser är militära styrkor verksamma på en annan stats territorium. De militära styrkornas ställning på en annan suverän stats territorium (värdstaten för insatsen) sköts med avtal mellan staterna. I avtalen bestäms det om styrkornas rättsliga ställning och immunitet på värdstatens territorium. Dessa avtal kallas avtal som reglerar den rättsliga ställningen för styrkorna (Status om Forces Agreement, SOFA-avtalet). I regel är det den som bemyndigat eller den som verkställer insatsen som ansvarar för förhandlingarna om SOFA-avtalen i förhållande till värdstaten. Vanligen riktar sig de förpliktelser som följer av avtalsarrangemangen, i praktiken att bevilja krishanteringsstyrkor dispens och privilegier, ensidigt till värdstaten. SOFA-avtalen ger inte upphov till befogenheter för styrkor som deltar i insatser. Befogenheterna följer av insatsens folkrättsliga mandat, den nationella lagstiftningen i de länder som sänder styrkor samt av militära order som ges vid insatsen.

Vid krishanteringsinsatser tjänstgör underrättelseenheterna eller underrättelseofficerarna i regel som en del av en nationell eller multinationell styrka. Underrättelseinhämtningen vid krishantering sker i regel i enlighet med bestämmelser och anvisningar från den organisation som leder insatsen. Verksamhetsmiljön och de insatsspecifika bestämmelserna ger upphov till mycket varierande krav på underrättelseinhämtningen. Inom krishanteringen ger den militära underrättelseinhämtningen de finländska krishanteringsstyrkorna kännedom om verksamhetsmiljön i verksamhetsområdet till stöd för nationellt beslutsfattande och krishanteringsstyrkornas egenskydd och planering av verksamheten. Syftet är dels att säkerställa krishanteringsstyrkornas egenskydd, dels att utveckla det nationella försvarets kapacitet.

*Radiosignalspaning*

Syftet med radiosignalspaning är att som en del av militär underrättelseinhämtning upprätthålla en lägesbild och ge förvarning. På kort sikt skapar radiosignalspaning en lägesbild över grupperingar, beredskap och verksamhet i fråga om de militära organisationer som övervakas. På lång sikt är det möjligt att med hjälp av radiosignalspaning följa hur den tekniska och operativa förmågan hos de organisationer som är föremål för spaningen utvecklas. Försvarsgrenarna och Försvarsmaktens underrättelsetjänst genomför signalspaning i form av underrättelseinhämtning på taktisk nivå.

Radiosignalspaning genomförs under normala förhållanden med de underrättelsesystem som finns inom landet eller på internationellt område. Underrättelseverksamhet i anslutning till Försvarsmaktens övningsverksamhet eller handräckningsuppdrag kan dessutom genomföras på en främmande stats territorium. Inhämtning av underrättelser i anslutning till krishanteringsuppdrag genomförs på det egna landets, mållandets eller tredjelandets territorium.

Radiosignalspaning riktas i enlighet med en plan för informationsinhämtning till sådana objekt utomlands som finns på målstatens territorium, på internationellt område eller på en tredjestats territorium. I exceptionella situationer såsom vid territoriekränkningar och störningar under normala förhållanden kan ett utländskt objekt finnas på och således också underrättelseinhämtningen rikta sig mot finska statens territorium.

Vid handräckningsuppdrag riktas radiosignalspaning mot alla behövliga objekt även på Finlands territorium. Med tanke på identifiering av särdragen hos identifieringsdatabaser och målsystem inom den militära underrättelseinhämtningen riktas underrättelseinhämtningen mot alla inhemska och utländska objekt.

I Finland indelas radiosignalspaningen på följande sätt:

Kommunikationssignalspaning som sker mot radiovågor (Communications Intelligence, COMINT) omfattar underrättelseinhämtning av olika typer av dataöverföringssignaler via radiovågor. Föremålet för underrättelseinhämtningen kan vara signalens informationsinnehåll, tekniska parametrar, signalkällans läge eller vilken information som helst som hänför sig till signalen och som producerar underrättelseinformation om den som använder signalen eller det system som använts.

Teknisk signalspaning (Electronic Intelligence, ELINT) omfattar underrättelseinhämtning via radiovågor från andra radiosändare än sådana som används för kommunikation, vanligen underrättelseinhämtning som inriktas på radarsändare och andra navigationssignaler. Genom underrättelseinhämtning via radarsignaler kan man t.ex. få reda på radarns läge, tekniska parametrar, typ av radar och radarns prestationsförmåga. På basis av dessa uppgifter kan man

t.ex. producera information om hot mot jaktplans och farkosters egenskyddssystem samt djupgående information om systemens prestationsförmåga. Teknisk signalspaning riktas inte mot kommunikation mellan personer.

Vid underrättelseinhämtning genom avlyssning av tekniska instrumenteringssignaler från främmande utrustning (Foreign instrumentation Signals Intelligence, FISINT) utnyttjas vanligtvis elektromagnetiska källor dvs. telemetrisignaler som används i rymdsystem, system ovan mark och undervattensystem. Föremål för underrättelseinhämtningen är sådana tekniska signaler mellan tekniska system som inte innehåller förtrolig kommunikation. Sådana källor omfattar styrsignaler från olika slags anordningar, t.ex. från robotar och flygplan. Av målsignalerna försöker man vanligen producera underrättelseinformation om målsystemets verksamhet och prestationsförmåga.

2.2.6 Försvarsmaktens informationsinhämtning utomlands

Det har inte föreskrivits särskilt om Försvarsmaktens informationsinhämtning utomlands. I viss mån har informationsinhämtningen ansetts grunda sig på Försvarsmaktens lagstadgade uppgifter. Försvarsmakten har utan uttryckliga bestämmelser utomlands kunnat använda sig av underrättelseinhämtning ur öppna källor, bildunderrättelser, geografisk underrättelseinhämtning, personbaserad underrättelseinhämtning i internationell verksamhet samt radiosignalspaning.

Försvarsmaktens hemliga inhämtande av information grundar sig starkt på utövande av befogenheterna för att förhindra och avslöja brott som avses i lagen om militär disciplin och brottsbekämpning inom försvarsmakten och på sådan assistans av polisen som avses i den lagen. Dessa befogenheter kan utövas endast på Finlands territorium.

Försvarsmaktens tillgång till information utomlands baserar sig dock i praktiken till största delen på Försvarsmaktens internationella underrättelsesamarbete, bevakning av öppna källor och försvarsattachéverksamheten.

Försvarsmakten har bedrivit omfattande bilateralt och multilateralt samarbete med utländska underrättelse- och säkerhetstjänster. Med hjälp av samarbetet säkerställs tillgången till utländska underrättelser som behövs för upprätthållandet av statens säkerhet. På grund av den allmänna utvecklingstrenden att säkerhetsfrågorna blir alltmer globala och den allt större betydelse som utländska underrättelser får till följd av det har Försvarsmakten under de senaste åren systematiskt utvidgat sitt internationella samarbetsnätverk.

Internationella samarbetsförfaranden som tjänar brottsbekämpning ska hållas åtskiljs från internationellt underrättelsesamarbete. Inom Försvarsmaktens verksamhetsområde har dessa liten betydelse.

Försvarsmakten bevakning av öppna källor när det gäller utlandet omfattar hela Försvarsmaktens verksamhetsområde. Uppgifter som inhämtats från öppna källor kombineras med uppgifter från andra källor i syfte att skapa en lägesbild av Finlands internationella säkerhetspolitiska miljö.

Som Försvarsmaktens informationsinhämtning som gäller utlandet betraktas dessutom verksamhet som sker med stöd av Wienkonventionen och som har beskrivits tidigare i denna proposition under rubriken personbaserad underrättelseinhämtning i internationell verksamhet.

2.2.7 Styrning av Försvarsmakten

Enligt 68 § 1 mom. i grundlagen, lagen om statsrådet (175/2003) och reglementet för statsrådet (262/2003) svarar försvarsministeriet för de ministerieuppgifter som gäller Försvarsmakten.

Utöver styrning av verksamheten svarar försvarsministeriet för Försvarsmaktens resultatstyrning och resurstilldelning. Försvarsmaktens informationsinhämtning har inte blivit ett eget moment separat från Försvarsmaktens omkostnadsmoment och ingen separat resultatmätare eller modell för resursfördelningen har införts i fråga om informationsinhämtningen.

Enligt 4 § i statsrådets förordning om försvarsministeriet (375/2003) föreskrivs det i ministeriets arbetsordning förutom om ministeriets uppgifter och utövande av beslutanderätt även om styrningen av ministeriets förvaltningsområde.

I 24 § i lagen om försvarsmakten konstateras det att Försvarsmakten lyder under försvarsministeriet. Styrningen av Försvarsmakten kan också behandlas i förberedande syfte vid ett gemensamt möte mellan republikens president och utrikes- och säkerhetspolitiska ministerutskottet. Bedömt som helhet är det fråga om en styr- och samordningsmekanism på statsrådsnivå. Bestämmelser om mekanismen har inte utfärdats på lagnivå.

Försvarsministern har det politiska ansvaret för Försvarsmaktens verksamhet och därför ska han eller hon vara medveten om de viktiga frågor som hör till Försvarsmaktens verksamhetsområde. Enligt 128 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten ska Försvarsmakten ge försvarsministeriet uppgifter om frågor med anknytning till försvarsmaktens brottsbekämpning vilka är samhälleligt eller ekonomiskt betydelsefulla eller tillräckligt allvarliga för att betraktas som betydelsefulla.

Försvarsmakten informerar republikens president, utrikes- och säkerhetspolitiska ministerutskottet samt riksdagens försvarsutskott och utrikesutskott för att hålla dem uppdaterade i frågor som gäller utrikes- och säkerhetspolitiken och säkerhetssituationen.

2.2.8 Ordnandet av militär underrättelseinhämtning

Den militära underrättelseinhämtningen indelas i tre nivåer: strategisk, operativ och taktisk. Med strategisk ledningsnivå avses den högsta statsledningen, dvs. riksdagen, republikens president och statsrådet.

Med strategisk militär ledning avses Försvarsmaktens överbefälhavare och kommendören för Försvarsmakten, vilkas uppgiftsområde omfattar militärpolitiska frågor och i synnerhet frågor som gäller användningen och ledningen av försvarssystemet.

Strategisk underrättelseinhämtning ger politiska och militära beslutsfattare omfattande kännedom om omvärlden på lång sikt och vid behov förvarning. Den strategiska underrättelseinhämtningen ska redan under normala förhållanden ge förvarning om betydande förändringar i staters och militära alliansers politik, militära åtgärder och betydande teknisk utveckling. Strategisk underrättelseinhämtning omfattar insamling, behandling, analys, produktifiering och distribution av uppgifter som behövs vid politisk beredning, drivande av politik och militär planering på nationell och internationell nivå samt ledning av underrättelseprocessen. När det gäller den strategiska underrättelseinhämtningen sker den viktigaste insamlingen genom den

militära underrättelseinhämtningen och den civila underrättelseinhämtningen. Även utrikesministeriet producerar information på strategisk nivå.

Den militära underrättelseinhämtningen svarar för sin del för att den strategiska militära ledningens kännedom om omvärlden upprätthålls på det sätt som det breda säkerhetsbegreppet avser och med betoning på militära uppgifter. Underrättelser som lämnas ut ska till innehåll och form tjäna detta.

Den operativa ledningsnivån inom den militära underrättelseinhämtningen omfattar i sin helhet Försvarsmakten, dvs. kommendören för Försvarsmakten, chefen för Huvudstaben, biträdande stabchefer, Huvudstaben, de inrättningar som är underställda Huvudstaben, Försvarshögskolan och försvarsgrenarna. Chefen för Huvudstabens underrättelseavdelning (nedan underrättelsechefen) är sektorchef med ansvarsområdet militär underrättelseinhämtning, och chefen för Försvarsmaktens underrättelsetjänst är direkt underställd honom eller henne. Underrättelsechefen, som lyder under Försvarsmaktens operationschef, leder den militära underrättelseverksamheten med bistånd av Huvudstabens underrättelseavdelning. Underrättelsechefen ger Försvarsmaktens underrättelseavdelning, försvargrenarna och andra inrättningar underställda Huvudstaben anvisningar om framställning av produkter för den militära underrättelseinhämtningen. Den militära underrättelseverksamheten omfattar som helhet frågor inom militär underrättelseinhämtning och militärt kontraspionage inklusive informationsinhämtning, behandling av information och rapportering.

Biträdande avdelningschef med ansvar för kontraspionage vid underrättelseavdelningen har självständiga befogenheter när det gäller förebyggande och avslöjande av brott och utövar då de befogenheter som har föreskrivits för en polisman som hör till befälet och för en anhållningsberättigad polisman i enlighet med 87 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Chefen för kontraspionage ansvarar för det säkerhetsdataregister och de temporära personregister som avses i lagen om militär disciplin och brottsbekämpning inom försvarsmakten.

Försvarsmaktens underrättelsetjänst är en militär inrättning underställd Huvudstaben som producerar de underrättelsetjänster som statsledningen och Försvarsmakten behöver. Inrättningen är en nationell aktör inom Försvarsmakten och svarar också för Försvarsmaktens geografiska information och information om förhållandena. Tiedustelukoulu är en skola som hör till inrättningen och ger fortbildning inom militär underrättelseverksamhet och inom säkerhetsområdet för Försvarsmaktens och de viktigaste samarbetsmyndigheternas personal. Till Försvarsmaktens underrättelsetjänsts funktioner hör inhämtning av information med olika former av underrättelseinhämtning samt analys och rapportering av inhämtad information.

Försvarsgrenarna, dvs. armén, marinen och flygvapnet, svarar för förvaltningen och användningen av övervakningssystemet samt producerar och bildar militära underrättelsestyrkor och underrättelseenheter på taktisk nivå som fungerar under undantagsförhållanden. Under normala förhållanden är den huvudsakliga uppgiften inom försvarsgrenarnas underrättelseinhämtning att bygga upp kapaciteten och upprätthålla beredskapen. Försvarsgrenarna deltar såväl under normala förhållanden som under undantagsförhållanden i den operativa verksamheten inom den militära underrättelseinhämtningen under ledning av Huvudstabens underrättelsechef. De svarar under undantagsförhållanden för produktionen och bildandet av behövliga underrättelsestyrkor. Försvarsgrenarnas övervakningssystem har till uppgift att producera och upprätthålla en sådan lägesbild över land- och havsområden och luftrummet i realtid som övervakningen och tryggandet av den regionala integriteten kräver. Försvarshögskolan och de

inrättningar som är underställda Huvudstaben stöder den militära underrättelseverksamheten med sin särskilda kompetens och förmåga.

2.2.9 Värnplikt och reservister

Enligt värnpliktslagen omfattar fullgörandet av värnplikten beväringstjänst, repetitionsövning, extra tjänstgöring och tjänstgöring under mobilisering. De värnpliktiga kan tjänstgöra eller höra till reserven eller den ersättande reserven. Också de personer som varit tvungna att avgå från en militär tjänst hör till reserven fram till utgången av det år under vilket de fyller 60 år.

Till repetitionsövning kan förordnas en värnpliktig som hör till reserven. Enligt värnpliktslagen kan vid reservens repetitionsövningar den militära kunskap och förmåga som inhämtats under beväringstjänsten upprätthållas samt utbildning för mera krävande uppgifter ges, de värnpliktiga göras förtrogna med de förändringar som utvecklingen inom det militära försvaret för med sig och en flexibel höjning av den militära beredskapen möjliggöras.

Enligt 102 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten kan de som hör till reserven och som fått tillräcklig utbildning användas för att förebygga och avslöja brott inom Försvarsmakten, när republikens president i enlighet med 83 § i värnpliktslagen har beslutat om extra tjänstgöring.

Enligt justitiekanslerns svar (OKV/50/20/2015) kan beväringar och andra tjänstgörande värnpliktiga användas i samband med att den militära beredskapen höjs. Då ska dock hänsyn tas till deras kunskaps- och färdighetsmässiga förutsättningar att sköta olika uppgifter. Bland annat ska det bedömas hur långt beväringen hunnit i sin utbildning eller hur lång tid det förflutit sedan reservisten fick sin utbildning.

En person som fått utbildning enligt värnpliktslagen och som ingått en särskild förbindelse kan anställas i anställningsförhållande enligt lagen om militär krishantering. En person som tjänstgöring enligt lagen om militär krishantering är enligt avtalet om krishanteringsoperationen underställd krishanteringsorganisationen och hans eller hennes rättigheter och skyldigheter bestäms därefter.

2.2.10 Rättslig övervakning av Försvarsmakten

2.2.10.1 Allmänt

Man strävar efter att säkerställa att Försvarsmaktens verksamhet är lagenlig genom såväl intern som extern övervakning. Vem som genomför övervakningen kan variera beroende på verksamhet eller ärende. Även befogenheterna för dem som genomför övervakning och de övervakningsmetoder som de har till sitt förfogande varierar.

Förhållandet mellan den interna och externa laglighetsövervakningen har t.ex. behandlats i Jaakko Jonkas utredning Poliisin johtamisjärjestelmä ja sisäinen laillisuusvalvonta (Polisens ledningssystem och interna laglighetsövervakning; Inrikesministeriets publikationer 48/2004). I utredningen konstateras det att den interna och externa övervakningen kompletterar varandra. Med tanke på trovärdigheten är den externa övervakningen viktig. Dessutom kan den kanske bättre avslöja vissa systemfel eller rättsligt ohållbar praxis hos organisationen. Även om den är effektiv kan den ändå avslöja och utreda enbart en del av felen. Ju närmare själva verksamheten övervakningen ligger, desto bättre blir dess felförebyggande effekt och

förmåga att upptäcka även ringa problem. Enligt utredningen bör också den interna laglighetsövervakningen ses som en del av den kvalitetsövervakning som åligger ledningen.

Lagenlighetens betydelse accentueras i Försvarsmaktens verksamhet jämfört med många andra verksamheter inom den offentliga sektorn. Försvarsmakten kan med stöd av lag såväl under normala förhållanden som under undantagsförhållanden ingripa i människors rättsliga intressen som skyddas som grundläggande fri- och rättigheter. Utomstående observatörers möjligheter att göra observationer av Försvarsmaktens verksamhet är ofta begränsade. På grund av verksamhetens särskilda omständigheter finns det inte heller alltid nödvändigtvis verklig möjlighet att göra observationer av verksamheten på objektet för åtgärderna. Vidare finns det inte alltid besvärsmöjlighet i fråga om militärmyndigheternas verksamhet (t.ex. militära kommandomål). En trovärdig laglighetsövervakning är viktig med tanke på förtroendet för myndighetsverksamheten. Den laglighetsövervakning som riktas mot Försvarsmaktens verksamhet delas in i extern laglighetsövervakning och intern laglighetsövervakning.

Myndigheternas interna övervakning och ledarskapet är viktiga med tanke på säkerställande av att verksamheten är lagenlig. Ju närmare verksamheten övervakningen ligger, desto bättre går det att observera och genast ingripa i även små problem. Även förvaltningsutskottet har i sitt utlåtande (FvUU 40/2014) konstaterat att inget system och ingen övervakning kan ersätta att saker och ting görs rätt från första början. Det är detta vi måste satsa på mer än något annat.

2.2.10.2 Försvarsmaktens interna laglighetsövervakning

Den interna laglighetsövervakningen riktas på ett mer heltäckande sätt än den externa övervakningen mot olika delområden inom Försvarsmaktens verksamhet. Den interna laglighetsövervakningen fungerar nära den konkreta praktiska verksamheten och i samarbete med dem som sköter uppgifter med anknytning till juridisk experthjälp. På det här sättet försöker man uppnå en tillräcklig förmåga att upptäcka objekt som kräver åtgärder inom laglighetsövervakningen.

Försvarsmaktens interna laglighetsövervakning kan delas in i två olika helheter. Laglighetsövervakningen genomförs i anknytning till ledningen av respektive förvaltningsenhet såsom allmän övervakning av verksamhetens lagenlighet. Det är varje chefs tjänsteplikt att ingripa i lagstridiga handlingssätt som en del av den dagliga ledningen av arbetet. Den interna övervakningen omfattar dessutom etisk utbildning i anslutning till personalens utbildning, övervakning som utförs av cheferna i samband med den dagliga verksamheten samt inbördes övervakning, arbetsordningar, operativa anvisningar och annan dokumentation.

Den andra helheten omfattar den särskilda laglighetsövervakning som Försvarsmaktens ledning utför och som enligt statsrådets förordning om försvarsmakten (1319/2007) hör till Försvarsmaktens assessor att sköta. Försvarsmaktens assessor leder och övervakar lagenligheten i Försvarsmaktens verksamhet samt den militära rättsvården. De viktigaste åtgärderna inom den interna laglighetsövervakningen bereds och läggs fram för assessorn av biträdande avdelningschef för Huvudstabens juridiska avdelning, sektorchefen för sektorn för laglighetsövervakning eller en militärjurist som sköter laglighetsövervakningsuppgifter. När det gäller det praktiska utförandet av laglighetsövervakningen är sektorn för laglighetsövervakning vid Huvudstabens juridiska avdelning en viktig aktör. Militärjuristerna inom det juridiska ansvarsområdet och truppförbandens rättsofficerare rapporterar till Huvudstabens juridiska avdelning om händelser i anslutning till laglighetsövervakningen.

Huvudstabens juridiska avdelning kan genomföra förfrågningar i anslutning till laglighetsövervakningen och på eget initiativ eller i samarbete med sina samarbetspartner göra behövliga undersökningar och utarbeta behövliga promemorior om ämnesområden som hör till laglighetsövervakningen. Huvudstabens juridiska avdelning kan behandla initiativ och frågor i anknytning till lagligheten som lämnas in av värnpliktiga, Försvarsmaktens personal eller andra. Huvudstabens juridiska avdelning kan utifrån sina observationer ta initiativ till ändring eller beredning av lagstiftning och administrativa bestämmelser och anvisningar.

De befogenheter som är jämförbara med de befogenheter som nu föreslås i regeringspropositionen hänför sig närmast till användning av hemliga metoder för inhämtande av information och hemliga tvångsmedel samt till övervakningsmekanismer som gäller dessa. Bestämmelser om övervakning av den militära underrättelseinhämtningen utfärdas separat till den del den gäller brottsbekämpning som utförs inom den militära underrättelseinhämtningen.

Enligt 129 § i lagen om militär disciplin och brottsbekämpning inom försvarmakten ger försvarsministeriet årligen riksdagens justitieombudsman en berättelse om användningen och övervakningen av hemliga tvångsmedel enligt lagens 37 § och hemliga metoder för inhämtande av information enligt lagens 89 § 1 mom. och om skyddandet av dem. Berättelsen ges dessutom till skyddspolisen för kännedom.

Enligt 127 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten övervakar Försvarsmaktens ledning brottsbekämpningen inom Försvarsmakten. Dessutom övervakar Försvarsmaktens assessor huvudstabens utredning av brott enligt 35 § i den lagen och avdelningschefen för underrättelseavdelningen förebyggandet och avslöjandet av brott enligt 86 § i den lagen.

Enligt 128 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten ska det protokoll som upprättas över användningen av hemliga tvångsmedel enligt 37 § och hemliga metoder för inhämtande av information enligt 89 § 1 mom. lämnas till försvarsministeriet. Försvarsministeriet ska dessutom ges uppgifter om frågor med anknytning till Försvarsmaktens brottsbekämpning vilka är samhälleligt eller ekonomiskt betydelsefulla eller tillräckligt allvarliga för att betraktas som betydelsefulla.

Det bör särskilt observeras att varje militär förman svarar för de uppgifter i anknytning till tillsynen över det disciplinära förfarandet som hör till honom eller henne enligt lagen om militär disciplin och brottsbekämpning inom försvarsmakten. I dessa uppgifter biträds disciplinära förmän av militärjurister och rättsofficerare. Den interna laglighetsövervakningen ska likaså skiljas från intern kontroll, vars syfte är att utvärdera och utveckla bl.a. hur effektiva riskhanterings-, övervaknings- samt lednings- och förvaltningsprocesserna är.

2.2.10.3 Försvarsmaktens externa laglighetsövervakning

*Laglighetsövervakning som utförs av Försvarsministeriet*

Enligt den laglighetsövervakning som definieras ovan kan försvarsministeriets övervakning av Försvarsmakten räknas som extern övervakning. Enligt 68 § i grundlagen svarar varje ministerium inom sitt ansvarsområde för beredningen av de ärenden som hör till statsrådet och för att förvaltningen fungerar som sig bör. Enligt 24 § 1 mom. i lagen om försvarsmakten lyder Försvarsmakten i administrativt avseende under försvarsministeriet. Enligt försvarsministeriets förordning om försvarsministeriets arbetsordning (1337/2011) har lagberednings- och rättsenheten som en uppgift att övervaka ministeriets och förvaltningsområdets laglighet samt ut-

veckla och samordna den. Direktören för lagberednings- och rättsenheten avgör de ärenden som gäller laglighetsövervakning. Betydande ärenden som gäller laglighetsövervakning avgörs dock av kanslichefen, om de inte på grund av sin samhälleliga eller ekonomiska betydelse kräver att ministern avgör dem.

I 128 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten finns bestämmelser om övervakning som försvarsministeriet utför. Enligt 129 § i samma lag ger försvarsministeriet årligen riksdagens justitieombudsman en berättelse om användningen och övervakningen av hemliga tvångsmedel enligt lagens 37 § och hemliga metoder för inhämtande av information enligt lagens 89 § 1 mom. och om skyddandet av dem. Berättelsen ges dessutom till skyddspolisen för kännedom.

*De högsta laglighetsövervakarna*

De högst laglighetsövervakarna, dvs. riksdagens justitieombudsman och justitiekanslern i statsrådet, ska bl.a. sköta uppgifter som gäller laglighetsövervakning som riktas mot Försvarsmakten.

I 108 § i grundlagen föreskrivs om justitiekanslerns uppgifter. Enligt grundlagen ska justitiekanslern bl.a. övervaka att domstolarna och andra myndigheter samt tjänstemännen, offentligt anställda arbetstagare och också andra, när de sköter offentliga uppdrag, följer lag och fullgör sina skyldigheter. Bestämmelser om riksdagens justitieombudsmans uppgifter finns till denna del på motsvarande sätt i 109 § i grundlagen. De högsta laglighetsövervakarna har i enlighet med 110 § i grundlagen åtalsrätt. Övervakarna kan utföra åtal eller förordna att åtal ska väckas. De högst laglighetsövervakarna har omfattande rätt att få upplysningar, vilket det föreskrivs om i 111 § i grundlagen.

Bestämmelser om justitiekanslern finns i lagen om justitiekanslern i statsrådet (193/2000). Liksom i fråga om riksdagens justitieombudsman omfattar justitiekanslerns viktigaste verksamhetsformer undersökning av klagomål, egna initiativ och granskningsverksamhet.

Närmare bestämmelser om riksdagens justitieombudsmans uppgifter finns i lagen om riksdagens justitieombudsman (197/2002). Som särskilt föremål för den övervakning som utförs av justitieombudsmannen anges behandlingen av beväringar och andra som fullgör militärtjänst samt krishanteringspersonalen. Enligt 5 § i den lagen gör justitieombudsmannen vid behov inspektioner för att göra sig förtrogen med angelägenheter som omfattas av justitieombudsmannens laglighetskontroll. Vid en inspektion har justitieombudsmannen rätt att få tillträde till alla den övervakades lokaler och tillgång till den övervakades alla datasystem samt enskilt samtala med inspektionsobjektets personal och med dem som tjänstgör eller är intagna där.

När det gäller de högsta laglighetsövervakarnas verksamhet ligger betoningen särskilt på övervakningen av grundläggande och mänskliga rättigheter. Inom laglighetsövervakningen fästs det allt mer vikt förutom vid övervakning av den formella lagenligheten också vid de faktiska konsekvenserna av tillämpningen av lagen. I riksdagens justitieombudsmans övervakning betonas för Försvarsmaktens del övervakning av hemliga tvångsmedel och hemliga metoder för inhämtande av information. De högsta laglighetsövervakarna har obegränsad rätt att av myndigheterna få de uppgifter som de behöver för sin övervakning.

De högsta laglighetsövervakarnas verksamhet ger för sin del trovärdighet för lagenligheten hos Försvarsmaktens verksamhet. Den externa laglighetsövervakningen ingriper bl.a. i uppen-

bara fel och ohållbara förfaranden. Den externa laglighetsövervakningen bedömer ur ett allmänt perspektiv ärenden som den fått för prövning och som den tagit upp för prövning.

*Nationella domstolar*

Försvarsmakten fattar förvaltningsbeslut inom många olika kategorier av ärenden. Ändring i ett beslut av Försvarsmakten får i regel sökas på det sätt som föreskrivs i förvaltningsprocesslagen (586/1996). På det här sättet deltar även förvaltningsdomstolarna för sin del de facto i Försvarsmaktens övervakning. När förvaltningsdomstolen säkerställer individens rättsskydd i förhållande till förvaltningsmyndigheterna, verkar den samtidigt som övervakare av lagenligheten i förvaltningen i ett enskilt fall. För Försvarsmaktens del kan frågor om handlingars offentlighet nämnas som en kategori av ärenden som omfattas av förvaltningsprocessen.

Allmänna domstolar har också beslutanderätt i fråga om vissa befogenheter som avses i 89 § 1 mom. i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. På det här sättet deltar de allmänna domstolarna i enskilda fall i övervakningen av lagenligheten av Försvarsmaktens åtgärder.

*Europeiska domstolar*

Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen) övervakar efterlevnaden av den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Europadomstolen kan också anses delta i övervakningen av att myndigheternas verksamhet är lagenlig när den avgör klagomål. Klagomål som riktas mot polisen utgör en mycket stor ärendekategori vid domstolen. Europadomstolen har under de senaste årtiondena avgjort även ett stort antal frågor som gällt säkerhetspolisen, säkerhetstjänster och underrättelsetjänster samt även hemliga tvångsmedel och hemliga metoder för inhämtande av information. I avgörandena har särskilt Europakonventionens artikel 8 om skydd för privatlivet och artikel 13 om effektiva rättsmedel tolkats. Tolkningen av Europakonventionen har stor betydelse för bedömningen av om underrättelseverksamheten är lagenlig och garantierna för rättsskyddet tillräckliga. Det är också fråga om Europadomstolens minimikrav på den nationella lagstiftningen.

EU-domstolen tolkar EU-lagstiftning och säkerställer att den tillämpas på samma sätt i alla EU-länder. EU-domstolen avgör också rättstvister mellan EU-länder och EU-institutioner. EU-domstolen har med anledning av artikel 4 (2) i fördraget om Europeiska unionens funktionssätt haft en ännu mer distanserad eller indirekt roll än Europadomstolen när det gäller övervakning av underrättelseverksamhet, men i vissa fall har dess förhandsavgöranden och talan om ogiltighetsförklaring av EU-lagstiftning betydelse även för underrättelseverksamheten och särskilt för utvecklandet av lagstiftningen om underrättelseinhämtning.

*Övervakning som dataombudsmannen utför*

Bestämmelser om dataombudsmannens uppgifter finns i lagen om datasekretessnämnden och dataombudsmannen (389/1994). Enligt 5 § i den lagen ska dataombudsmannen behandla och avgöra ärenden som gäller behandling av personuppgifter och kreditupplysningar så som föreskrivs i personuppgiftslagen (523/1999) och kreditupplysningslagen (527/2007) samt sköta övriga uppgifter som följer av de nämnda lagarna. Dataombudsmannen ska också följa den allmänna utvecklingen i fråga om behandlingen av dessa uppgifter samt ta nödvändiga initiativ. Dessutom ska dataombudsmannen sköta den informationsverksamhet som hör till ombudsmannens verksamhetsområde samt det internationella samarbete som har samband med

behandlingen av personuppgifter. I praktiken ger dataombudsmannen allmän handledning och rådgivning samt samarbetar med olika intressegrupper, avgör ärenden, övervakar och granskar samt ska höras och ge utlåtanden, informera och delta i internationellt samarbete. Försvarsmaktens informationssystem omfattas till stor del av den så kallade indirekta rätten till insyn (45 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet). Dataombudsmannen har årligen gjort mellan en och tio granskningar av Försvarsmakten huvudsakligen på basis av begäran om granskning. Under ett besök har behandlingen av personuppgifterna för flera personer som lämnat begäran om granskning granskats.

2.2.11 Bekämpning av hot mot informationssäkerhet

Kommunikationsverkets Cybersäkerhetscenter är en nationell myndighet för informationssäkerhet som bl.a. förebygger, samlar in uppgifter om och utreder sådana kränkningar av informationssäkerheten som hänför sig till kommunikationsnät och som därigenom riktar sig mot finländska aktörer samt informerar om betydande hot mot informationssäkerheten. Enligt cybersäkerhetsstrategin ska Cybersäkerhetscentret också producera och upprätthålla en sammanställd lägesbild över cybersäkerheten. Cybersäkerhetscentret samlar in information om it-incidenter och förmedlar den till olika aktörer samt utformar och delar ut den sammanställda lägesbilden över cybersäkerheten. Cybersäkerhetscentrets kunder kan utnyttja lägesbildsinformationen för sina egna beredskapsarrangemang och prioriteringar.

Vid utformningen av lägesbilden utnyttjas utöver nationella källor även Cybersäkerhetscentrets internationella samarbetsnätverk som grundar sig på frivillighet och ömsesidigt förtroende. Moderorganisationer i de GovCert-grupper som hör till samarbetsnätverket finns inom olika funktioner inom statsförvaltningen i sina egna länder. Till exempel Sveriges CERT-SE är en del av Myndigheten för samhällsskydd och beredskap, medan Tysklands CERT-BUND verkar inom inrikesministeriets förvaltningsområde. I vissa stater finns CERT-grupperna inom försvarsministeriets förvaltningsområde och i andra stater är de en del av underrättelsemyndigheterna (Government Communications Headquarters, GCHQ).

Bestämmelser om rätt att vidta åtgärder för att sörja för informationssäkerheten finns i 272 § i informationssamhällsbalken. Bestämmelsen ger företag, sammanslutningar och myndigheter verktyg för att upptäcka och avvärja cybergärningar som riktar sig mot dem. Åtgärderna för upptäckande vidtas decentraliserat, varvid deras kvalitet och nivå varierar från organisation till organisation. Informationssamhällsbalkens 272 § samt 20 § i dess föregångare, lagen om dataskydd vid elektronisk kommunikation (516/2004), har gjort det möjligt att utveckla också ett centraliserat system för upptäckande av hot mot informationssäkerheten (HAVARO-systemet) i syfte att skydda de mest betydande aktörerna med tanke på samhällets övergripande säkerhet. HAVARO är ett system för upptäckande av och varning för kränkningar av informationssäkerheten som Kommunikationsverkets Cybersäkerhetscenter erbjuder sådana företag och aktörer inom statsförvaltningen som är kritiska med tanke på försörjningsberedskapen.

Syftet med HAVARO-systemet är att med hjälp av olika unika signaturer identifiera skadlig nättrafik och avancerade nätangrepp som äventyrar informationssäkerheten (Advanced Persisten Threat, allmänt APT). Ett annat syfte med systemet är att stödja skapandet av en bättre lägesbild av de hot mot informationssäkerheten som riktar sig mot finländska datanät. Med hjälp av denna information strävar man efter att i ett så tidigt skede som möjligt upptäcka fenomen som påverkar informationssäkerheten, för att behövliga skyddsåtgärder ska kunna inledas i tid och riktas rätt. De unika signaturer som identifierar sabotageprogram och som ska utnyttjas i systemet grundar sig huvudsakligen på information som Cybersäkerhetscentret fått av inhemska och utländska samarbetspartner.

För statsförvaltningen erbjuds med stöd av GovHAVARO motsvarande tjänster för övervakning av datanät i syfte att upptäcka och avvärja hot mot informationssäkerheten.

Automatisk analys av innehållet i kommunikationen riktas mot innehållet i alla meddelanden som kommer in i eller sänds ut från datanätet eller datasystemet hos den som använder sig av automatisk analys. Det huvudsakliga syftet med analysen är att upptäcka sabotageprogrammens försök till intrång i datasystemet samt den kommunikation som sabotageprogram som eventuellt redan finns i systemet för med sina värdar.

Sabotageprogram och kommandon identifieras i ett första skede vid automatisk analys av innehållet utifrån på förhand fastställda definitioner, 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 informationssamhällsbalken företaget, sammanslutningen eller myndigheten att behandla innehållet i meddelandet manuellt.

Finland är som informationssamhälle och som ekonomi som stöder sig på internationella marknader beroende av att informationsinfrastukturen fungerar utan störningar. Välfungerande och tillförlitliga kommunikationsnät och kommunikationstjänster är viktiga med tanke på Finlands ekonomiska tillväxt, konkurrenskraft, innovationer och välfärd inom samhällets alla sektorer.

Funktionssäkerheten i informationsinfrastrukturen är viktig också med tanke på den övergripande säkerheten i samhället. Att samhället blir allt mer it-baserat, att det utländska ägandet i telekommunikationsinfrastrukturen ökar och att datatekniska verksamheter inom statsförvaltningen läggs ut på entreprenad ställer nya slags krav när det gäller tryggandet av samhällets vitala funktioner. Med samhällets vitala funktioner avses förvaltningsövergripande, för samhället nödvändiga funktioner som ska vara tryggade i alla situationer. Dåligt fungerande datatekniska system, kollaps för informationsinfrastrukturen och olika slag av hot mot informationssäkerheten inverkar negativt på de offentliga tjänsterna, affärslivet, förvaltningen och således på hela samhället. Största delen av Finlands kritiska telekommunikationsinfrastruktur och dess tjänster ägs och produceras av den privata sektorn, och därför är dess betydelse vid tryggandet av samhällets vitala funktioner viktig.

Att den elektroniska kommunikationen samt datanäten och datasystemen fungerar väl och inte utsätts för störningar skyddas med hjälp av informationssäkerheten. Med informationssäkerhet avses administrativa och tekniska åtgärder genom vilka det säkerställs att endast de som har rätt att använda uppgifterna har tillgång till dem (konfidentialitet), att uppgifterna inte kan ändras av andra än de som har rätt att göra det (integritet) och att uppgifterna och datasystemen kan utnyttjas av dem som har rätt att använda dem (lättillgänglighet).

De som använder elektroniska kommunikationsnät och kommunikationstjänster sköter om sin informationssäkerhet på olika sätt. Informationssäkerheten kan skötas t.ex. med dataadministrativa metoder eller genom att införa tekniska begränsningar för användningen av kommunikationsnätet eller tjänsten. Statsförvaltningens enhetliga natur gör det möjligt att styra förvaltningens informationssäkerhet på ett centraliserat sätt och med stöd av enhetliga principer. Finansministeriet styr och leder det allmänna utvecklandet av den offentliga förvaltningens informationssäkerhet samt statsförvaltningens informationssäkerhet och ICT-beredskapen. Finansministeriets styrande uppgift grundar sig bl.a. på lagen om styrning av informationsförvaltningen inom den offentliga förvaltningen (634/2011) och på 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 föreskrivs om säkerhetsnätet (TUVE), som i samma telekommunikationsnät sammanför statens ledning, ministerierna, Försvarsmakten, gränsbevakningssektionen, polisen och räddningsväsendet.

Den offentliga förvaltningens säkerhetsnät erbjuder alla användare och deras viktigaste tjänsteproducenter en stabil data- och kommunikationsteknisk tjänstemiljö. Säkerhetsnätets datakommunikations- och dataskyddslösningar gör det möjligt att införa olika skyddsnivåer samt gemensamma eller separata databehandlingsmiljöer för användarna. Syftet med detta är att på ett kostnadseffektivt sätt åstadkomma ett för myndigheterna gemensamt och samverkande datanät som täcker hela landet och som fungerar tillförlitligt också under undantagsförhållanden och när bl.a. naturfenomen, elavbrott och de ständigt ökande attackerna mot datanät inträffar. Finansministeriet fattar under normala förhållanden och vid störningar under normala förhållanden beslut om den prioritet, skyndsamhet och övriga viktighetsklassificering som gäller för säkerhetsnätets tjänsteproduktion och användning.

Finansministeriet inledde under 2013 också ett projekt för att utveckla statens dataskyddsverksamhet dygnet runt (SecICT). Projektet har till uppgift att planera och inrätta en myndighetsfunktion för att förebygga och samordna omfattande och allvarliga störningar i informationssäkerheten. Inom ramen för projektet breddas och utvecklas tjänster som förbättrar statsförvaltningens informationssäkerhet. Inom projektet startar också grupper som har till uppgift att åtgärda störningar (VIRT-funktion) samt utvecklas det operativa tjänster som stöder hanteringen av störningar (GovSOC-tjänster). Utvecklandet görs i samarbete med statens och den privata sektorns aktörer inom data- och cybersäkerhet samt pilotorganisationer. Avsikten var att projektet skulle slutföras vid utgången av 2016.

Inom den privata sektorn är det inte möjligt att styra informationssäkerheten på ett centraliserat sätt, utan nivån på informationssäkerheten och de lösningar som valts för att upprätthålla informationssäkerheten varierar enligt varje organisations egna behov och betoningar. Upptäckt av hot mot informationssäkerheten och skyddet mot dem baserar sig såväl inom förvaltningen som även inom den privata sektorn i praktiken på kommersiella informationssäkerhetsprogram och informationssäkerhetstjänster. En del av statsförvaltningen och de företag som är kritiska med tanke på försörjningsberedskapen utnyttjar vid skyddet även HAVARO-systemet.

### 2.3 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU

#### 2.3.1 Internationella konventioner om mänskliga rättigheter

##### 2.3.1.1 Förenta nationernas konvention om medborgerliga och politiska rättigheter

Internationella konventionen om medborgerliga och politiska rättigheter, som antogs av FN:s generalförsamling 1966 (den s.k. MP-konventionen, FördrS 8/1976) 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, ej heller för olagliga angrepp på sin heder och sitt anseende. Dessutom har envar rätt till lagens skydd mot sådana ingripanden eller angrepp. Avvikelse från skyldigheten enligt artikeln får göras endast under allmänt nödläge, som hotar nationens fortbestånd och som officiellt kungjorts som sådant.

Det förbud att ingripa i privatliv och korrespondens som anges i artikel 17 i MP-konventionen är inte absolut, utan förbudet gäller ”godtyckligt” och ”olagligt” ingripande i rättigheter. Konventionsstaterna kan i sin nationella lagstiftning föreskriva om de situationer som berättigar till ett ingripande och om de metoder som ska användas vid ingripandet. Alla konventionsstater har föreskrivit om ingripande i rättigheter som görs i syfte att bekämpa brott och flera av dem också om ingripande i rättigheter som görs i syfte att upprätthålla den nationella säkerheten.

Genomförandet av MP-konventionen övervakas av FN:s kommitté för de mänskliga rättigheterna, som kontinuerligt utvecklar tolkningen av bestämmelserna i konventionen. I kommitténs allmänna kommentar nr 16 från 1988 (A/43/20) tolkas innehållet i artikel 17 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 för 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 fastställs 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 klagomål om kränkning av artikel 17 som gäller integritetsskydd har lämnats in med stöd av det fakultativa protokollet till MP-konventionen, men kommittén har hittills inte behandlat frågor med anknytning till it-säkerhet och elektronisk kommunikation. Det kan anses sannolikt att frågor med anknytning till den elektroniska kommunikationens konfidentialitet kommer att bli mera synliga i det arbete som kommittén för de mänskliga rättigheterna bedriver.

2.3.1.2 Europakonventionen

Vid bedömning av om det ska tillåtas att det föreskrivs om befogenheter för militär underrättelseinhämtning är Europakonventionen (FördrS 63/1999), som ingicks inom Europarådet år 1950 och som Finland anslöt sig till 1989, av större praktisk betydelse än MP-konventionen. Efterlevnaden av Europakonventionen övervakas av Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen), som i detta syfte behandlar och avgör klagomål som gäller brott mot konventionen. Europadomstolen har i många avgöranden tagit ställning till hur rätten till skydd för förtroligt meddelande enligt Europakonventionen ska tolkas. Flera av dessa avgöranden gäller elektronisk kommunikation och några underrättelseinhämtning som avser datatrafik eller därmed jämförbara former av myndighetsverksamhet.

*Skydd för privatlivet (artikel 8 i Europakonventionen)*

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 konventionen är denna rätt dock inte obegränsad, eftersom myndigheterna får ingripa i den när lagen tillåter detta 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 eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Enligt Europadomstolens vedertagna avgörandepraxis inbegriper begreppen privatliv och korrespondens, vilka nämns i artikel 8(1) i Europakonventionen, 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). Såväl kommunikationens innehåll som kommunikationens identifieringsuppgifter omfattas av skyddet (bl.a. Malone mot Förenade kungariket, Weber och Saravia mot Tyskland, P.G. och J.H. mot Förenade kungariket). I fråga om identifieringsuppgifterna har Europadomstolen särskilt konstaterat att uppgifter t.ex. om de telefonnummer som en person har kommunicerat till utgör en organisk del av kommunikationen. Överlämnandet även av sådana uppgifter till en myndighet utan samtycke av personen i fråga utgör ingripande i dennes privatliv (Malone mot Förenade kungariket).

Myndigheten behöver de facto inte behandla uppgifterna för att det ska vara fråga om ingripande i privatliv, utan som ingripande ska betraktas redan det att myndigheten samlar in och sparar dem för senare användning (Marper mot Förenade kungariket). Enbart det att sådan lagstiftning existerar som gör det möjligt att hemligt observera kommunikationsförbindelser, ingriper i de rättigheter som artikel 8 i Europakonventionen garanterar parterna i kommunikationen och även potentiella parter (Klass mot Tyskland, Liberty m.fl. mot Förenade kungariket). Övervakningens potentiella objekt måste då ha sådan rätt till ett effektivt rättsmedel inför en nationell myndighet som garanteras i artikel 13 i Europakonventionen. Enligt den artikeln ska var och en, vars i konventionen 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.

Även om sannolikheten för hemlig övervakning av en person är liten, måste han eller hon kunna få sitt påstående om att rättigheterna enligt artikel 8 i Europakonventionen har blivit kränkta prövat vid Europadomstolen, om effektiva nationella rättsmedel saknas (Kennedy mot Förenade kungariket).

Av det att både kommunikationens innehåll och identifieringsuppgifter omfattas av skyddet enligt artikel 8 i Europakonventionen följer inte att myndigheterna inte kan ingripa i dem. Ingripandet i privatlivet kan vara jämförelsevis vittomfattande när det sker inom ramen för artikel 8 i Europakonventionen. Artikel 8 i konventionen ställer tre villkor för att man i myndighetsverksamhet ska kunna ingripa i de rättigheter som garanteras i artikeln: 1) ingripandet ska vara tillåtet med stöd av nationell lag, 2) ingripandet ska ske för att trygga vissa intressen som särskilt räknas upp i artikeln och 3) ingripandet ska vara nödvändigt i ett demokratiskt samhälle. Ett av de intressen som möjliggör ingripande i skyddet för privatliv och därmed också i skyddet för konfidentiell kommunikation är den nationella säkerheten.

Ingripande i de rättigheter som garanteras i artikel 8 i Europakonventionen ska grunda sig på nationell lag. Detta kravs betydelse framhävs i synnerhet då man ingriper i rättigheter i hemlighet för den som är föremål för ingripandet. Gränserna för myndigheternas prövningsrätt och sätten att utöva prövningsrätten ska tillräckligt tydligt anges i lag för att den möjlighet till god-

tycke som ingår i hemligt utövande av de verkställande befogenheterna ska kunna avvärjas (Malone mot Förenade kungariket, Amann mot Schweiz, Telegraaf Media Nederland Landelijke Media B.V. m.fl. mot Nederländerna, Rotaru mot Rumänien).

Europadomstolen har i sina avgöranden upprepade gånger betonat att en lag som möjliggör hemliga myndighetsåtgärder och ingriper i skyddet för privatlivet ska vara förenlig med rättsstatsprinciperna, tillgänglig för medborgarna och till sin art sådan att medborgarna kan förutse vilka följder tillämpningen av den får för dem själva (bl.a. Kruslin mot Frankrike, Huvig mot Frankrike, Lambert mot Frankrike). Lagen ska vara tillräckligt tydlig (”sufficiently clear in its term”) så att den på ett tillräckligt sätt visar (”an adequate indication”) under vilka förhållanden och under vilka förutsättningar medborgarna kan bli föremål för hemliga myndighetsåtgärder (Kopp mot Tyskland, Kruslin mot Franskrike, Huvig mot Frankrike). Lagen får inte vara sådan att den möjliggör att hemlig observation riktas slumpmässigt mot vem som helst (Amann mot Schweiz).

När det bedöms om kravet på förutsebarhet uppfylls ska vid sidan av den egentliga lag som folkrepresentationen stiftat även förordningar och myndighetsföreskrifter beaktas. De t.o.m. mycket allmänna bestämmelser som ingår i den egentliga lagen kan preciseras med instrument på lägre nivå. Dessa ska dock offentliggöras – sådana interna myndighetsföreskrifter som inte är tillgängliga för medborgarna uppfyller inte kravet på förutsebarhet (bl.a. Silver m.fl. mot Förenade kungariket, Malone mot Förenade kungariket). Den allmänt tillgängliga lagen ska definiera åtminstone arten och omfattningen av de observationsbefogenheter som ska utövas i hemlighet, de personkategorier som befogenheterna får utövas mot, arten av den verksamhet som ger anledning till att utöva befogenheterna, de förfaranden som ska följas när den information som inhämtas med hjälp av befogenheterna undersöks, utnyttjas, sparas, distribueras vidare och undanröjs samt övervakningen av befogenheterna och rättsmedel som gäller dessa (Amann mot Schwiz, Valenzuela Contreras mot Spanien, Prado Bugallo mot Spanien, Shimovolos mot Ryssland). De krav som ska ställas på att lagstiftningen är förutsebar gäller oberoende av om det är fråga om observation som grundar sig på brott och som gäller enskilda personers kommunikationsförbindelser eller sådan storskalig allmän övervakning av kommunikationsförbindelser som grundar sig på hot (Weber och Saravia mot Tyskland, Liberty m.fl. mot Förenade kungariket).

Europadomstolen har i två viktiga avgöranden bedömt hur väl den storskaliga allmänna övervakningen av internationella kommunikationsförbindelser överensstämt med Europakonventionen. I fallet Liberty m.fl. mot Förenade kungariket ansåg domstolen att den nationella lagstiftning som möjliggjorde allmän övervakning till sin art var sådan att den inte uppfyllde kravet i artikel 8(2) i Europakonventionen på att hemlig observation ska grunda sig på 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 fallet Liberty m.fl. mot Förenade kungariket var det fråga om en storskalig övervakning av utrikes telefontrafik. Övervakningen utfördes av signalspaningsverket, som lyder under försvarsministeriet i Storbritannien, och inom ramen för den kunde man samtidigt avlyssna t.o.m. 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 inrikta inhämtande av information på kommunikationsförbindelser mellan Storbritannien och utlandet. I tillstånden definierades de kommunikationsförbindelser som inhämtande av information kunde riktas mot på en mycket allmän nivå (t.ex. alla meddelanden som förmedlas via sjökablar mellan Storbritannien och det övriga Europa). I samband med att

tillstånd beviljades skulle inrikesministern definiera vilket material inhämtandet av information gällde. 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 brottslig verksamhet eller för att trygga landets ekonomiska intressen. När tillstånd beviljades skulle inrikesministern också meddela sådana sekretessbelagda föreskrifter som han eller hon ansåg behövliga 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 föreskrifters innehåll eller område. Efter att säkerhetsmyndigheterna fått tillstånd av inrikesministern utformade de självständigt de automatiska sökbegrepp med hjälp av vilka den information som gällde den nationella säkerheten eller andra i lagen nämnda intressen filtrerades ur den totala mängden kommunikation. Säkerhetsmyndigheterna hade sina egna interna föreskrifter om på vilka grunder de uppgifter som erhölls som resultat av filtreringen skulle behandlas, sparas, delas och undanröjas, men dessa föreskrifter var inte offentliga eller allmänt tillgängliga.

I sitt avgörande i saken konstaterade Europadomstolen att inrikesministerns tillståndsbeslut enligt lagen kunde omfatta vilket meddelande som helst, vilket gjorde att vilket som helst meddelande som vem som helst skickat till eller fått från utlandet hade kunnat fångas upp. Följaktligen hade den verkställande makten i själva verket beviljats obegränsad prövningsrätt när det gällde att fånga upp utländska meddelanden. Lagen medgav också en omfattande prövningsrätt i fråga om vilka meddelanden som faktiskt granskades. I detta hänseende var det tillräckligt att inrikesministern ansåg granskningen behövlig 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 inrikesministerns föreskrifter i saken var inte offentliga. Sammanfattningsvis konstaterade Europadomstolen att gränserna för den mycket vida prövningsrätt som beviljats för infångandet och granskningen av meddelanden inte hade angetts tillräckligt tydligt för den verkställande makten. I synnerhet hade det inte angetts offentligt hur gallringen, användningen, förvaringen och förstöringen av infångat material skulle genomföras. Således motsvarade Storbritanniens signalspaningslagstiftning inte kvalitetskraven enligt artikel 8(2) i Europakonventionen, och europakonventionen hade överträtts.

I fallet Weber och Saravia mot Tyskland var det fråga om storskalig s.k. strategisk övervakning som Tysklands underrättelsetjänst BND hade bedrivit i fråga om mobiltelefontrafiken mellan Tyskland och utlandet, vilket det hade föreskrivits om i nationell lag. Enligt denna lag fick strategisk övervakning av mobiltelefontrafiken bedrivas för att avvärja vissa särskilda hot som riktade sig mot den nationella säkerheten. Sådana i lagen definierade hot var militära attacker som riktades mot Tyskland, terrordåd som skulle genomföras i Tyskland och som till sin karaktär var internationella, internationell smuggling av vapen, storskalig import av narkotika, penningförfalskning utomlands och penningtvätt med anknytning till ovannämnda fenomen. Tillstånd till varje enskilt strategiskt övervakningsuppdrag beviljades av förbundsstatens minister efter att han eller hon först hört det parlamentariska övervakningsorganet. 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. Lagen innehöll bestämmelser om hur det material som hade filtrerats skulle behandlas och i vilka fall sådana uppgifter om personer som dykt upp genom filtreringen fick användas för att förebygga, avslöja och reda ut brott. Likaså innehöll lagen bestämmelser om när den filtrerade informationen skulle betraktas som irrelevant och hur man skulle förfara med sådan information. Vidare föreskrevs det i lagen om giltighetstiderna för övervakningstillstånden, hur länge

filtrerade uppgifter skulle bevaras, om förstörande av uppgifter samt om grunderna och förutsättningarna för att lämna ut uppgifterna till andra myndigheter.

Europadomstolen ansåg att Tysklands lagstiftning uppfyllde de krav på kvalitet och förutsebarhet som ska ställas på lag enligt artikel 8 i Europakonventionen. Viktigt i detta hänseende var bl.a. det att lagen definierade de hot som skulle avvärjas för att övervakning skulle få bedrivas. Lagen ansågs också erbjuda en tillräcklig anvisning om vilka personkategorier övervakningen enligt lagen kunde riktas mot. De automatiska sökbegrepp som skulle användas för att inrikta övervakningen skulle direkt med stöd av lagen framgå av de tillstånd som beviljats för övervakningen, varvid den myndighet som bedriver övervakning inte har obegränsad prövningsrätt när det gäller att definiera dem. Med tanke på att kravet på förutsebarhet skulle uppfyllas var det också av betydelse att lagen definierade maximala giltighetstider för tillstånden och innehöll bestämmelser om de förfaranden som skulle följas när uppgifterna granskades och utnyttjades. Likaså var det enligt Europadomstolen av betydelse att lagen föreskrev om de begränsningar och villkor som skulle följas vid vidareöverlåtelse av uppgifter samt om de förhållanden under vilka uppgifterna skulle förstöras. I sitt avgörande i fallet Weber och Saravia konstaterade Europadomstolen även särskilt att den allmänna övervakningen av kommunikationsförbindelser på tysk mark i princip inte kan kränka andra länders statssuveränitet fastän den andra parten i kommunikationsförbindelserna skulle befinna sig i ett sådant annat land.

Den nationella säkerheten är ett av de intressen som enligt artikel 8(2) i Europakonventionen kan berättiga till att ingripa i skyddet för privatlivet. Europadomstolen har i sin rättspraxis endast sällan ifrågasatt de svarande staternas påståenden om att ingripandet har skett med hänsyn till den nationella säkerheten. Det verkar som om staterna har en synnerligen bred prövningsmarginal vad gäller hurdan verksamhet de anser att äventyrar den nationella säkerheten och därmed kan berättiga till ett ingripande i de rättigheter som garanteras i artikel 8 i Europakonventionen. Bakom detta ligger att den nationella säkerheten av tradition omfattas av staternas suveränitet (Bucur och Toma mot Rumänien). På basis av Europadomstolens avgörandepraxis står det klart att åtminstone det militära försvaret och bekämpningen av terrorism och av olovlig underrättelseverksamhet hör till den nationella säkerheten (bl.a. Klass mot Tyskland, Weber och Saravia mot Tyskland). Den nationella säkerheten kan emellertid utsättas för många slags hot som är svåra att förutse eller definiera på förhand. Av detta följer att klargörandet av begreppet i första hand måste överlåtas åt nationell praxis (Kennedy mot Förenade kungariket). Staternas prövningsrätt kan för sin del ökas av det att den nationella säkerhetens gräns mot andra tillåtna grunder (bl.a. allmän säkerhet och förhindrande av oordning eller brottslighet) att ingripa i de rättigheter som garanteras i artikel 8(1) i Europakonventionen kan uppfattas som varierande från fall till fall.

Det tredje villkoret för att myndigheterna ska få ingripa i de rättigheter som artikel 8 i Europakonventionen garanterar är att ingripandet är nödvändigt i ett demokratiskt samhälle i syfte att skydda demokratiska institutioner och den mycket viktiga information som erhålls är absolut nödvändig för en underrättelseinsats. Tröskeln för hemligt inhämtande av information ska alltid vara hög. Systemen måste byggas upp så att de används sparsamt och endast i verkligt väl motiverade fall. Modeller där myndigheterna ges för stor prövningsrätt är enligt Europadomstolens åsikt alltid utsatta för missbruk och är således inte förenliga med kraven i Europakonventionen (Szabó och Vissy mot Ungern).

Kravet på nödvändigt i ett demokratiskt samhälle inbegriper att ingripandet i rättigheter ska svara mot ett tvingande samhälleligt behov (”correspond to a pressing social need”). Av kravet följer också att ingripandet ska vara förenligt med proportionalitetsprincipen: Ingripandet ska stå i ett förnuftigt förhållande till det syfte som tillåts i artikel 8(2) i Europakonventionen och

som åberopas som berättigande grund (bl.a. Gillow mot Förenade kungariket, Silver m.fl. mot Förenade kungariket, Handyside mot Förenade kungariket).

Bedömningen av om ett ingripande är nödvändigt såväl med tanke på ett samhälleligt behovs tvingande natur som också med tanke på proportionaliteten hör i första hand eller åtminstone i ett första skede till den nationella lagstiftarens eller de nationella myndigheternas uppgifter (Silver m.fl. mot Förenade kungariket, Handyside mot Förenade kungariket). När denna bedömning görs har de nationella aktörerna ett visst utrymme för sin prövning, vars omfattning bestäms bl.a. av vilken av de rättigheter som garanteras i Europakonventionen ingripandet gäller, hur långtgående ingripande det är fråga om, samt vilket av de i artikel 8(2) i Europakonventionen tillåtna syftena som utgör den grund som berättigar till ingripandet. Det finns mer utrymmer för prövning när den berättigande grunden är den nationella säkerheten (Klass m.fl. mot Tyskland, Leander mot Sverige). I frågor som gäller den nationella säkerheten gäller statens ganska omfattande prövningsrätt också de konkreta verktyg och metoder med hjälp av vilka den skyddar intresset i fråga. I sitt avgörande Weber och Saravia mot Tyskland ansåg Europadomstolen att staten inom ramen för sin prövningsrätt kunde föreskriva om storskalig övervakning av kommunikationsförbindelser som en metod för att skydda sin nationella säkerhet. Det var fråga om ett nödvändigt ingripande i ett demokratiskt samhälle i rättigheter som artikel 8 i Europakonventionen garanterar för enskilda rättssubjekt.

Europadomstolen har dessutom fäst uppmärksamhet vid övervakningssystem som riktar sig mot hemliga metoder för inhämtande av information. I synnerhet övervakningens effektivitet och övervakningsorganens oberoende har lyfts fram som viktiga krav. Övervakningens effektivitet har samband med frågor om tillsynsmyndighetens rätt att få information och om anmälan om att befogenheterna använts till den som varit föremål för dem. De krav på oberoende som Europadomstolen ställer har inte uppfyllts t.ex. i system där övervakaren har ett nära förhållande till den verkställande makten. Även alltför nära politiska kopplingar utgör tecken på att övervakningssystemet inte är tillräckligt oberoende. Även om Europadomstolen betonar att övervakningen inte behöver utföras av domstolar, har vikt fästs vid yrkeskvalifikationerna hos ledamöterna i organen, och i argumentationen har den yrkesmässiga bakgrunden för dem som utsetts till uppdraget beaktats. Europadomstolen har förhållit sig positiv till övervakningsmodeller där den som utsetts till uppdraget förutsätts ha en hög domarbefattning (Szabó och Vissy, Dumitru Popescu mot Rumänien nr 2).

Avgöranden av dem som utför laglighetsövervakning bör ha en juridiskt bindande verkan i förhållande till dem som övervakas. Med tanke på skyddande av demokratin är det inte tillräckligt att laglighetsövervakarna kan styra dem som de övervakar med hjälp av rekommendationer (Segerstedt-Wiberg m.fl. mot Sverige). Den juridiska reglering som gäller hemliga befogenheter ska vara offentlig och så exakt att laglighetsövervakningen kan utföras på ett trovärdigt sätt (Liberty m.fl. mot Förenade kungariket), dock utan att syftet med hemligt inhämtande av information äventyras (Segerstedt-Wiberg m.fl. mot Sverige). Med tanke på skyddandet av demokratin är det också av betydelse att folkrepresentationen för sin del deltar i övervakningen av de hemliga observationsbefogenheterna (Campbell mot Förenade kungariket, Leander mot Sverige).

När det gäller Europadomstolens senare avgörandepraxis kan man lyfta fram avgörandet i målet Roman Zakharov mot Ryssland, där Europadomstolen konstaterade att hemlig underrättelseverksamhet hade kränkt de mänskliga rättigheterna. Klaganden framförde att tre telefonoperatörer hade kränkt skyddet för privatlivet. Bakgrunden till avgörandet var bl.a. två rättsliga beslut, vilka gav operatörerna rätt till olovlig avlyssning i efterhand samt till ett tillägg till operatörernas standardavtal enligt vilket abonnemanget kan stängas av och samtalsuppgifterna

lämnas till brottsbekämpande myndigheter, om telefonen användes som medel för terroristhot. Enligt Europadomstolen var den nationella lagstiftningen inte tillräckligt detaljerad för att skydda klagandens rätt till privatliv. Rättsmedlen kan i praktiken inte garanteras om de som är föremål för övervakningen i regel inte informeras om hemligt inhämtande av information eller om personerna efter att de informerats på begäran inte får information om övervakningen. Europadomstolen ansåg att det för att rättsmedlen ska garanteras är nödvändigt att informera dem som är föremål för övervakningen om övervakningen och ge dem information i anknytning till den, när detta inte längre äventyrar syftet med övervakningen. Anmärkningsvärt i detta fall var att Europadomstolen tog saken till behandling trots att klaganden inte ens påstod sig ha blivit utsatt för kränkning.

*Rätt till ett effektivt rättsmedel (artikel 13 i Europakonventionen)*

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

Artikel 13 i konventionen avviker till sin natur från ovan beskrivna artikel 8, eftersom artikel 13 alltid kommer att ha koppling till andra rättigheter och friheter i Europakonventionen. Artikel 8 gäller självständig rätt, medan artikel 13 granskas endast i förhållande till en konventionsbestämmelse som definierar någon annan rättighet. Artikel 13 kompletterar de artiklar i konventionen som definierar de materiella mänskliga rättigheter som tryggas i konventionen genom att förutsätta effektiva inomstatliga rättsmedel med tanke på kränkningar av dessa rättigheter. Således, om klagandens påstående inte omfattas av tillämpningsområdet för Europakonventionen, har det inte heller kunnat ske någon kränkning av artikel 13.

Konventionsbestämmelsen kan betraktas som ett uttryck för att även de mänskliga rättigheter som skyddas genom internationella avtal även på processuell nivå i första hand ska tryggas inom ramen för den nationella rättsordningen. Medlemsstaterna har makt att bestämma på vilket sätt det sätter i kraft kraven i artikel 13. Artikel 13 förutsätter inte att det finns sådana rättsmedel med vilka det nationellt kan prövas om den nationella lagstiftningen är förenlig med Europakonventionen. Europadomstolen har tillämpat denna princip på fall där man haft för avsikt att bestrida antingen en viss norm i en lagstiftning eller mer allmänt läget för den nationella lagstiftningen.

Att artikel 13 om rättsmedel i regel inte är tillämplig i fråga om artiklarna om rättegångsförfarande har samband med att till skillnad från artikel 5 (rätt till frihet och säkerhet) och artikel 6 (rätt till en rättvis rättegång) kräver artikel 13 inte nödvändigtvis att det effektiva rättsmedel som avses i artikeln är en domstol. Snarare är det fråga om arten av rättighet och det beror på omständigheterna i varje enskilt fall hurdant nationellt rättsskydd som artikel 13 kan anses förutsätta. Bestämmelsen i artikel 13 kräver rättsmedel, men garanterar inte klaganden ett positivt slutresultat i själva sakfrågan. Effektiviteten bedöms också i första hand huruvida organet i fråga är behörigt att avgöra saken och hurdana processuella rättssäkerhetsgarantier organet kan erbjuda vad gäller processen. Staterna har omfattande prövningsrätt när det gäller hur de ska uppfylla kraven på effektivt rättsmedel. Av staterna krävs det endast att de i sin rättsordning tryggar innehållet i de rättigheter som avses i Europakonventionen.

Europadomstolen har betonat att det vid tolkningen av artikel 13 ska lämnas visst utrymme för flexibilitet i det enskilda fallet och att överdriven formalitet ska undvikas. Omständigheterna i varje enskilt fall har betydelse för Europadomstolens helhetsbedömning, där de formella förut-

sättningarna enligt den nationella lagstiftningen och statens rättsliga och politiska systems realiteter och klagandes individuella situation beaktas. Av artikel 13 följer inte heller att den inomstatliga instans där ändring sökts uttryckligen ska kunna pröva ett påstående om överträdelse av någon annan bestämmelse i Europakonventionen. Det räcker att det finns ett rättsmedel genom vilket en fråga om överträdelse av konventionen sakligt har kunnat föras till prövning.

Tillämpningsområdet för artikel 13 i Europakonventionen begränsar sig endast till fall där klaganden har faktiskt behov av rättsskydd i fråga om det rättigheter som tryggas i Europakonventionen. Enligt Europadomstolens avgörandepraxis medför ett påstående som kan motiveras (”arguable claim”) och som gäller kränkning av en rättighet som tryggas i Europakonventionen en skyldighet att garantera ett rättsmedel enligt artikel 13 för den som utsatts för den påstådda kränkningen. Om någon t.ex. anser att hans eller hennes privatliv har kränkts i strid med artikel 8, ska den nationella rätten erbjuda ett effektivt rättsmedel för en sådan påstådd kränkning, förutom om påståendet inte kan motiveras. Även om tillsynsorganen oberoende av om påståendet är motiverat eller inte slutligen inte heller anser att artikel 8 har kränkts, kan avsaknaden av nationellt rättsmedel innebära en kränkning av artikel 13. Huruvida påståendet är motiverat kan för sin del avgöras i varje enskilt fall utifrån fallets särdrag. I avgörandet Powell och Rayner mot Förenade kungariket (1990) uttryckte Europadomstolen som sin ståndpunkt, som numera ska anses vedertagen, att man i bakgrunden till ett klagomål som lämnats utan prövning såsom uppenbart omotiverat inte kan tänka att det finns ett på sådant sätt motiverat påstående att staten skulle vara skyldig att garantera ett rättsmedel enligt artikel 13.

Förutsättningen för att få en sak prövad i Europadomstolen är att de nationella rättsmedlen har uttömts. Om ett effektivt rättsmedel helt och hållet saknas, är klaganden inte skyldig att utnyttja rättsmedel på nationell nivå. Det står alltså klart att om ett nationellt rättsmedel helt saknas leder det till kränkning av artikel 13. Så här var det t.ex. när det nationella systemet inte garanterade något rättsmedel för avlyssning av arbetsplatsens telefon (Halford mot Förenade kungariket 1997).

I fråga om artikel 8 i Europakonventionen har Europadomstolen konstaterat att rättsmedlen ska vara så effektiva som möjligt. I avgörandet Klass m.fl. mot Förbundsrepubliken Tyskland (1978), som gällde telefonavlyssning, konstaterade Europadomstolen att ”effective remedy” i ett sådant fall betyder ett så effektivt rättsmedel som möjligt med beaktande av de begränsningar som naturligt följer av hemlig övervakning. Under dessa förhållanden har den i praktiken till sin betydelse begränsade möjligheten för en person som känner sig övervakad att vädja till en särskild kommission som övervakar verkställandet av lagen och till författningsdomstolen ansetts tillräcklig med tanke på artikel 13. I senare rättspraxis har Europadomstolen ansett att så länge tvångsmedlen hålls hemliga är det med tanke på artikel 13 tillräckligt att det enbart finns en objektiv kontrollmekanism, såsom nationell besvärsmöjlighet, men så fort ett sådant tvångsmedel kommer fram i ett konkret fall, ska den som blivit föremål för det ha tillräckliga rättsmedel till sitt förfogande.

Ett rättsmedel är ineffektivt när den instans som avgör saken inte är behörig att fatta bindande beslut. I bakgrunden till fallet Leander mot Sverige (1987) fanns det ett kartotek som säkerhetspolisen i Sverige hade och med stöd av vars uppgifter personer som klassats som säkerhetshot kunde förvägras inträde till vissa statliga tjänster eller uppdrag. Enligt Sveriges regering hade personen fyra rättsmedel: 1) möjlighet att söka tjänsten och lämna in klagomål till regeringen, 2) möjlighet att begära tillstånd av polisstyrelsen att ta del av uppgifter om sig själv samt få ett avslagsbeslut i detta avseende i sista hand prövat hos Regeringsrätten, 3) möj-

lighet lämna in klagomål till justitieombudsmannen, 4) möjlighet att lämna in klagomål till justitiekanslern. Europadomstolen ansåg med rösterna 4–3 att inget av dessa var ett sådant effektivt rättsmedel som avses i artikel 13, men med beaktande av sakens natur kunde dessa och den möjlighet som klaganden utnyttjade att lämna in klagomål till regeringen om polisstyrelsens åtgärder sammantagna anses som tillräckliga. För att komma fram till detta resultat betonade Europadomstolen även den parlamentariska kontroll som hänför sig till Sveriges system. Ovan beskrivna sammantagna verkan av rättsmedlen kan vara tillräcklig särskilt i situationer som gäller statens säkerhet.

Däremot slogs det fast att en kränkning av artikel 13 hade skett i fallet Segerstedt-Wiberg mot Sverige (2006). Även om domen inte kullkastar de principer som utvecklades i Leander-avgörandet, visar den ett mer kritiskt förhållningssätt till den uppfattningen att rättsmedlen som helhet när de granskas tillsammans kan vara tillräckliga i en situation där inte ett enda rättsmedel i sig självt är ett effektivt rättsmedel, och med själva rättsmedlet vill man uppnå ett mer konkret resultat. Rättsskyddet kan också vara ineffektivt om den instans som avgör målet inte är behörig att döma ut skadestånd till klaganden.

Staten kan inte åberopa nationell säkerhet som grund för ingripande i rättsmedel som avses i artikel 13 annat än i undantagsfall. I fallet Smith och Grady mot Förenade kungariket godkände Europadomstolen inte statens påstående om att förbudet för homosexuella att tjänstgöra i armén tjänade kraven på nationell säkerhet. Europadomstolen slog fast att det skett en kränkning av artikel 13, eftersom de rättsmedel som fanns var för svaga och hindrade en effektiv prövning av synpunkterna i artikel 8.

Fallet Al-Nashif mot Bulgarien (2002) gällde utvisning av utlänning av skäl som hänförde sig till statens säkerhet. Klaganden åberopade skäl med anledning av vilka artikel 13 blev tillämplig med avseende på skyddet av familjelivet enligt artikel 8. Även om en parts rätt att ta del av allt bakgrundsmaterial i sitt fall kan begränsas med anledning av statens säkerhetsintressen, måste en oberoende instans i sådana fall bedöma om grunderna för förfarandet är lämpliga och säkerställa att det kontradiktoriska förfarandet genomförs i tillräcklig utsträckning. Eftersom den behöriga domstolen i fallet inte hade någon möjlighet att pröva grunderna för myndighetens beslut, ansågs det att artikel 13 hade kränkts. Motsvarande konstellation kom upp även i fallet C.G. m.fl. mot Bulgarien (2008). I det fallet grundade sig utvisningen på inrikesministeriets hemliga rapport enligt vilken klaganden på basis av underrättelser hade deltagit i narkotikabrott. Domstolar som senare behandlade målet hade nog fått kännedom om rapporten, men de nöjde sig med uppgifterna i rapporten utan att vidta några andra åtgärder för att utreda fakta i ärendet och utan att ge klaganden effektiva möjligheter att bestrida korrektheten av innehållet i den hemliga rapporten eller möjlighet att argumentera med stöd av de grunder som hänför sig till skyddet för familjelivet. Även i detta fall ansågs rättsmedlet strida mot artikel 13.

Högst förvaltningsdomstolen i Finland hänvisade bl.a. till domen i målet Al-Nashif i flera av sina beslut sommaren 2007, i vilka frågan gällde partsoffentlighet i fråga om utlåtanden som ingår i skyddspolisens säkerhetsriskbedömning i ärenden som gäller familjeåterförening enligt utlänningslagen och medborgarskapsansökningar. Högst förvaltningsdomstolen ansåg att utlåtandena bör hemlighållas för parterna, men för att garantera ett rättvist förfarande krävdes det att domstolen fick kännedom om grunderna för ett negativt utlåtande för parten och att domstolen tog ställning till om dessa grunder var korrekta.

Huruvida ett effektivt rättsmedel är förenligt med artikel 13 är inte beroende av om användningen av rättsmedlet har varit framgångsrik. I fallet Vereinigung Demokratischer Soldaten Österreichs och Gubi mot Österrike (1994) var det fråga om ett förbud i anslutning till artikel

10 mot att sprida en dagstidning i ett kasernområde. I detta fall ansågs staten bära bevisbördan för att de rättsmedel som finns är effektiva. Regeringen visade inte att den klagande föreningen hade ett effektivt rättsmedel till sitt förfogande, och därför ansågs det att en kränkning av artikel 13 hade skett. Däremot kunde den beväring som var den andra klaganden lämna in klagomål om kränkning av sin yttrandefrihet till författningsdomstolen, vilket han också gjorde. Det att klagomålet inte ledde till resultat hade ingen betydelse med tanke på artikel 13, så till denna del hade ingen kränkning skett.

Europadomstolen har i senare rättspraxis krävt effektiva rättsmedel även i fråga om laglighetskontrollen av tvångsmedel som ingriper i hemfriden. I fallet Stefanov mot Bulgarien (2008) bedömdes rättssäkerhetsgarantier i fråga om hemfriden med tanke på kraven i artikel 13. I det fallet gav den nationella lagstiftningen inte möjlighet till domstolskontroll av grunderna för husrannsakan eller av det sätt på vilket husrannsakan genomfördes. Artikel 13 i Europakonventionen förutsätter inte att rättsmedlet ska finnas till förfogande före husrannsakan. En kränkning av artikel 13 följde dock av det att man inom det nationella rättssystemet inte kände till något annat rättsligt förfarande inom ramen för vilket den person som var föremål för husrannsakan hade kunna bestrida lagligheten av husrannsakan och beslag och få lämplig gottgörelse i det fall att beslutet om husrannsakan och beslag eller verkställandet av dem skulle ha skett olagligen.

Ett rättsmedel är inte effektivt om klaganden inte har den rätt att klaga som det krävs att klaganden har (locus standi). Vanligen förutsätts det att den person som är föremål för en påstådd kränkning har direkt tillgång till rättsmedel utan några mellanhänder. Rättsmedlet ska i praktiken vara tillgängligt och sådant att domstolen kan ingripa i den påstådda kränkningen. Till exempel i fallet Smith och Grady mot Förenade kungariket (1999) kunde de nationella domstolarna ingripa endast i några delar av påstådda kränkningar av privatlivet, dock utan att kunna göra en bedömning enligt artikel 8 av om ingripandet är berättigat och proportionerligt.

Rättsmedlets effektivitet förutsätter verkställighet av beslutet. Att ändringssökandet är framgångsrikt är inte i sig tillräckligt för att göra rättsmedlet förenligt med artikel 13, om domstolsavgörandet eller något annat beslut inte har några konkreta följder. Rättsmedlet är inte effektivt, om myndighetens åtgärder eller försummelser hindrar användningen av det. Så är det t.ex. när klaganden av domstolen har fått ett föreläggande, som myndigheterna dock inte iakttar. När det i fråga om vissa länder upprepade gånger framkommit betydande förseningar av verkställigheten av nationella domstolars domar och beslut, har Europadomstolen i sin rättspraxis betonat att de nationella rättssystemen ska ha tillräckliga rättsskyddsgarantier även mot förseningar av detta slag.

Europadomstolen har i många av sina tidigare avgöranden tagit ställning till frågan om en person som är föremål för informationsinhämtning bör och i vilka situationer i så fall ha rätt att av myndigheten få kännedom om en informationsinhämtningsåtgärd som har inriktats på personen. I fallen Klass mot Tyskland och Weber & Saravia mot Tyskland ansåg Europadomstolen att lagstiftningen enligt vilken den som är föremål för informationsinhämtning genast skulle underrättas när detta inte längre äventyrade informationsinhämtningens syfte var godtagbar med tanke på Europakonventionen. Europadomstolen fäste också vikt vid att bedömningen av om det föreligger förutsättningar att underrätta eller låta bli att underrätta inom Tysklands system hörde till ett oberoende organs (G10-kommissionen) uppgifter, inte till säkerhetsmyndigheten.

I fallen Association for European Integration and Human Rights and Ekimdzhiev mot Bulgarien och Dumitru Popescu mot Rumäninen konstaterade Europadomstolen att nationell lag-

stiftning enligt vilken den som är föremål för informationsinhämtning inte alls behöver underrättas normalt strider mot Europakonventionen. Vid bedömning av Rysslands lagstiftning (Zakharov mot Ryssland) konstaterade Europadomstolen att lagstiftningen inte i något som helst fall krävde att föremålet för informationsinhämtningen behövde underrättas. Föremålet för informationsinhämtningen hade möjlighet att få kännedom om informationsinhämtning som inriktats på honom eller henne endast i det fall att åtal väcktes mot honom eller henne. Eftersom största delen av de personer som varit föremål för informationsinhämtning således aldrig fick kännedom om den informationsinhämtning som riktats mot dem kunde det inte heller söka rättsskydd mot lagstridig myndighetsverksamhet. Den möjlighet att lämna in klagomål som Rysslands lagstiftning i och för sig medgav förutsatte att klaganden exakt kunde identifiera det beslut som klagomålet gällde, vilket naturligtvis inte var möjligt om personen inte alls var medveten om beslutets existens. På basis av det ovan beskrivna ansåg Europadomstolen att Rysslands lag inte innehöll bestämmelser om sådana effektiva rättsmedel som förutsätts i artikel 13 i Europakonventionen.

Förutsättningen ”nödvändigt i ett demokratiskt samhälle” har också samband också med kravet på tillgång till rättsskydd på nationell nivå. Konventionsstatens domstol eller något annat motsvarande organ ska åtminstone i efterhand kunna säkerställa att ingripandet i de rättigheter som avses i artikel 8 i Europakonventionen i ett enskilt fall var proportionerligt och nödvändigt. Detta innebär att den person som är föremål för informationsinhämtning ska kunna anföra besvär eller klagomål om informationsinhämtningsåtgärder som inriktats på honom eller henne.

En förutsättning för att använda besvärs- eller klagomålsmöjligheten är i allmänhet att personen av myndigheten blir underrättad om informationsinhämtning som riktats mot honom eller henne efter att användningen av metoden för informationsinhämtning har avslutats (se ovan Zakharov mot Ryssland). Av detta följer emellertid inte att personen måste underrättas omedelbart efter att informationsinhämtningen har avslutats. Ett hot, som man har inhämtat information om med hjälp av en metod för underrättelseinhämtning, kan fortgå i åratal eller till och med i decennier, varvid det är nödvändigt att skjuta upp underrättandet i motsvarande grad för att skydda säkerhetsmyndigheternas verksamhet. För att möjliggöra användning av ett rättsmedel ska underrättandet dock göras efter att det inte längre finns någon individuell grund för att avstå från att underrätta (Klass mot Tyskland, Zakharov mot Ryssland). Ett system som över huvud taget inte förutsätter att den person som är föremål för en åtgärd underrättas kan dock också vara förenligt med Europakonventionen. Då bör rätten att anföra klagomål ha tagits in i den nationella lagstiftningen på en så allmän nivå att vem som helst kan anföra klagomål enbart på den grunden att personen misstänker att myndigheterna har ingripit i det skydd som personens förtroliga kommunikation åtnjuter (Kennedy mot Förenade Kungariket).

2.3.1.3 Europeiska unionens stadga om de grundläggande rättigheterna

Europeiska unionens stadga om de grundläggande rättigheterna, som trädde i kraft 2009, definierar de grundläggande rättigheter som gäller på unionsnivå. Medlemsstaterna är skyldiga att iaktta stadgan om de grundläggande rättigheterna alltid när 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 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 innehåller bestämmelser om de i stadgan tryggade grundläggande rättigheternas räckvidd. 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 artikel 52.3 finns bestämmelser om att 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 ha samma innebörd och räckvidd som i konventionen. Denna bestämmelse hindrar dock inte unionsrätten från att tillförsäkra ett mer långtgående skydd.

Av artikel 52.3 i stadgan följer att innehållet i artikel 7 i stadgan motsvarar innehållet i artikel 8 i Europakonventionen. I ingressen till stadgan anges särskilt att de rättigheter som bekräftas i stadgan har sin grund förutom i Europakonventionen även i rättspraxis vid Europadomstolen. Europadomstolens omfattande avgörandepraxis som gäller artikel 8 i Europakonventionen ska således anses ha relevans också för tolkningen av artikel 7 i stadgan.

Trots det som sägs ovan är det inte Europadomstolen utan EU-domstolen och nationella domstolar som svarar för övervakningen av respekten för de grundläggande rättigheterna enligt stadgan. Med tanke på underrättelseinhämtning som avser datatrafik är den dom som EU-domstolen gav i april 2014 och genom vilken domstolen ogiltigförklarade datalagringsdirektivet från 2006 av betydelse. Direktivet hade ålagt unionens medlemsstater skyldighet att föreskriva om omfattande lagring av teleidentifieringsuppgifter med tanke på bekämpning och utredning av allvarliga brott.

EU-domstolen ansåg i ovannämnda dom att datalagringsdirektivet stred mot proportionalitetsprincipen i artikel 52.1 i stadgan. Proportionalitetsprincipen inbegriper att en begränsning av en grundläggande rättighet är nödvändig. När EU-domstolen bedömde hur nödvändig den begränsning av rättigheterna som gjordes i datalagringsdirektivet var fäste domstolen vikt vid att skyldigheten enligt direktivet att lagra teleidentifieringsuppgifter omfattade alla personer, alla elektroniska kommunikationssätt och så gott som alla identifieringsuppgifter utan någon som helst åtskillnad, begränsning eller undantag som skulle ha baserat sig på målet att förhindra allvarlig brottslighet. Lagringsskyldigheten omfattade också alla sådana personers teleidentifieringsuppgifter i fråga om vilka det inte fanns något bevis ens för avlägsen eller indirekt koppling till brottslighet. Således måste det anses att direktivet i praktiken ingrep i rättigheterna för varje person som vistades inom EU.

Enligt EU-domstolen borde direktivet ha innehållit åtminstone en del av följande element för att det skulle ha varit förenligt med proportionalitetsprincipen:

Något slags objektiva gränser med anknytning till direktivets mål i fråga om vilka personers teleidentifieringsuppgifter som får lagras.

En mer exakt definiering av de brott som skulle bekämpas eller utredas för att myndigheterna skulle få ta del av och använda de lagrade teleidentifieringsuppgifterna. Till denna del hänvisar direktivet endast till ”allvarliga brott”, vars innehåll bestäms enligt varje medlemsstats nationella lagstiftning.

Materiella och processuella förutsättningar för att ta del av och använda uppgifterna. I direktivet förutsattes t.ex. inte något tillstånd av domstol eller något annat oberoende organ för att få

ta del av uppgifterna, utan frågan om förfarandet har fått regleras i den nationella lagstiftningen.

Närmare bestämmelser om lagringstiderna för identifieringsuppgifter. I direktivet föreskrivs att uppgifterna ska lagras i minst sex månader utan att det görs någon skillnad på om uppgifterna kan vara till nytta vid brottsbekämpning eller inte.

I syfte att säkerställa ett effektivt dataskydd tillräcklig garantier för att de uppgifter som ska lagras inte missbrukas. Direktivet tillåter att teleföretagen beaktar ekonomiska aspekter när de fastställer den skyddsnivå de tillämpar.

Bestämmelser om att uppgifterna ska lagras inom unionens territorium.

Riksdagens grundlagsutskott har i sitt utlåtande GrUU 18/2014 rd framfört kommentarer om den dom som EU-domstolen gav. 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 borde ha innehållit 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 inse att EU-domstolens dom inte egentligen skapar någon ny rätt. Det motsvarar Europadomstolens vedertagna avgörandepraxis. Europadomstolen har meddelat ett stort antal avgöranden där den på motsvarande sätt som i EU-domstolens dom, men mer detaljerat, har behandlat de element som en lag som ingriper i skyddet för privatlivet måste innehålla för att överrensstämma med proportionalitetsprincipen och vara förutseende. De viktigaste i detta avseende är Europadomstolens avgöranden som direkt gäller underrättelseinhämtning som avser datatrafik eller närliggande fenomen, Klass mot Tyskland (1978), Weber och Saravia mot Tyskland (2006) och Liberty m.fl. mot Förenade kungariket (2008).

EU-domstolen har dryftat vilken inverkan artiklarna 7, 8 och 47 i stadgan har på ett mål där det var fråga om överföring av personuppgifter till ett tredjeland mot vilket det hade framförts invändningar i fråga om dataskyddets tillräckliga nivå (Schrems mot Data Protection Commissioner). Målet bottnar i en oro för Förenta staternas underrättelseinhämtning, med anledning av vilket Schrems den 25 juni 2013 lämnade in ett klagomål till dataombudsmannen i Irland där han gjorde gällande att Förenta staternas rätt och praxis inte garanterade något reellt skydd mot statlig övervakning för uppgifter som lagrades i Förenta staterna. På basis av domen upphävdes kommissionens beslut 2000/520/EG, där kommissionen bl.a. hade konstaterat att den skyddsnivå enligt safe harbour-systemet som Förenta staterna garanterar för överförda personuppgifter och som i praktiken hindrar de nationella tillsynsmyndigheterna från att utreda om nivån är tillräcklig och vid behov avbryta överföringen av uppgifter är adekvat. Safe harbour-systemet innehåller ett antal principer för skydd av personuppgifter som amerikanska företag frivilligt kan förplikta sig att följa.

I sin dom ansåg EU-domstolen att det aktuella beslutet av kommissionen inte kan omintetgöra befogenheter som de nationella tillsynsmyndigheterna har med stöd av stadgan och dataskyddsdirektivet (95/46/EG). EU-domstolen framhöll i detta sammanhang den rätt till skydd för personuppgifter som garanteras i stadgan och den uppgift som tillsynsmyndigheterna åläggs i enlighet med stadgan.

Vad gäller en skyddsnivå som väsentligen är likvärdig med den som garanteras för de grundläggande fri- och rättigheterna inom unionen konstaterade EU-domstolen att enligt unionsrätten är en lagstiftning inte är begränsad till vad som är strängt nödvändigt när den generellt tillåter lagring av samtliga personuppgifter om alla personer vilkas uppgifter har överförts från unionen till Förenta staterna, utan att det görs några skillnader, begränsningar eller undantag med beaktande av det eftersträvade syftet och utan att det föreskrivs något objektivt kriterium som gör det möjligt att avgränsa myndigheternas åtkomst till uppgifterna och att avgränsa den senare användningen av uppgifterna. Lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer anses kränka det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet. EU-domstolen ansåg likaså med hänvisning till artikel 47 i stadgan 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 kränker det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, eftersom möjligheten i fråga är en grundförutsättning för en rättsstat. Slutligen konstaterade EU-domstolen att kommissionens beslut av den 26 juli 2000 berövar de nationella tillsynsmyndigheterna de befogenheter de har, när en person ifrågasätter huruvida ett beslut är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter. Kommissionen har inte haft befogenheter att inskränka de nationella tillsynsmyndigheternas befogenheter på sätt som skett.

Av ovannämnda skäl förklarade EU-domstolen kommissionens beslut av den 26 juli 2000 ogiltigt. Till följd av domen är Irlands tillsynsmyndighet skyldig att med vederbörlig omsorg utreda Schrems klagomål. Av denna anledning gav en arbetsgrupp enligt artikel 29 i dataskyddsdirektivet den 16 oktober 2015 ett yttrande om verkningarna av Schrems-domen. Arbetsgruppen ansåg det viktigt att tillsynsmyndigheterna har en gemensam ståndpunkt för tillämpningen av domen. Arbetsgruppen uppmanade medlemsstaterna och EU:s institutioner att inleda en diskussion med Förenta staternas myndigheter i syfte att hitta en sådan lösning som på ett heltäckande sätt och med respekt för de grundläggande rättigheterna möjliggör överföring av uppgifter till Förenta staterna. Arbetsgruppen fortsätter bedömningen av verkningarna av EU-domstolens dom på andra sätt att överföra uppgifter och konstaterar att man tills vidare kan använda standardavtalsklausuler för överföring av personuppgifter samt bindande företagsregler (Binding Corporate Rules). Arbetsgruppen påpekar dock att detta inte hindrar dataskyddsmyndigheter från att utreda enskilda fall, t.ex. klagomål, och utöva sina befogenheter för att skydda enskilda personer.

Som resultat av förhandlingarna efter det att domen meddelats enades EU och Förenta staterna om Privacy Shield-systemet, som ersatte Safe Harbour och infördes den 1 augusti 2016.

Det tidigare Safe Harbour-systemet innehöll sju grundläggande principer som även inkluderats i Privacy Shield. Dessa principer är information till enskilda personer, valfrihet, begränsning av vidareöverföring av uppgifter, informationssäkerhet, ändamålsbegränsning, krav på uppgifternas riktighet samt rättsmedel. Privacy Shield förbättrar dock enskilda personers möjligheter att få tillgång till rättsmedel och få ersättning för dataskyddsintrång. Dessutom begränsar den rätten för organisationer verksamma i Förenta staterna att lämna vidare uppgifter till tredje

parter. Organisationer inom Privacy Shield-systemet kan t.ex. inte i någon omfattande grad lämna ut de uppgifter de behandlat till myndigheter i Förenta staterna.

Liksom tidigare är det fortfarande möjligt att överföra personuppgifter från EU till Förenta staterna bl.a. med uttryckligt samtycke av den person uppgifterna gäller, med stöd av särskilda avtal som garanterar dataskyddsnivån eller med stöd av BCR-regler som gäller företag. I och med införandet av Privacy Shield-systemet ska organisationerna dock bedöma om de av alla alternativ som står till buds använder sig av det allra mest ändamålsenliga sättet för att överföra personuppgifter från EU till Förenta staterna.

EU-domstolen ansåg i sin dom i de förenade målen Tele2 Sverige och Watson (C-203/15 och C-697/15) att generell och odifferentierad lagring av alla trafikuppgifter och lokaliseringsuppgifter avseende elektroniska kommunikationsmedel inte är förenlig med unionsrätten (punkterna 103 och 105). Den nationella lagstiftning som det är fråga om i målet syftade till att införliva datalagringsdirektivet, som EU-domstolen dock förklarade ogiltigt genom ovan beskrivna Digital Rights Ireland-domen.

Även om en generell och odifferentierad lagring av alla uppgifter enligt EU-domstolen inte är förenlig med proportionalitetsprincipen, kan medlemsstaterna dock föreskriva om riktad lagring av dessa uppgifter och om behöriga nationella myndigheters rätt att få tillgång till sådana uppgifter i syfte att uppfylla ett berättigat mål som nämns i direktivet om integritet och elektronisk kommunikation och under förutsättning att bestämmelserna är tydliga och precisa och att lagringen av och tillgången till dessa uppgifter i enlighet med proportionalitetsprincipen har begränsats till vad som är strängt nödvändigt (punkterna 94–96, 103, 108, 109, 116).

I direktivet om integritet och elektronisk kommunikation anges uttryckligen att bl.a. statens verksamhet på straffrättens område och verksamheter som avser allmän säkerhet och försvar inte omfattas av direktivets tillämpningsområde, men i det möjliggörs lagstiftningsåtgärder som hänför sig till uppfyllandet av dessa mål eller som tjänar dessa mål. Dessa åtgärder anses således höra till direktivets tillämpningsområde (punkterna 69–76). EU-domstolen fäste i sin bedömning av detta vikt vid att tjänsteleverantörer som direktivet avser vidtar åtgärder och fullgör skyldigheter genom vilka direktivets ändamålsenliga verkan tryggas.

Även om förutsättningarna för lagring och användning av uppgifter kan variera i medlemsstaternas olika nationella lagstiftning, räknade domstolen ändå upp flera materiella och formella aspekter som måste beaktas i fråga om sådana bestämmelser. Bestämmelserna ska för det första möjliggöra lämpliga rättsmedel. Uppgifter som enligt bestämmelserna ska lagras ska uppfylla objektiva grunder och de ska ha ett nära samband med det eftersträvade syftet. Omfattningen och tillämpligheten av bestämmelserna kan begränsas till vad som är strängt nödvändigt även genom villkor som gäller bl.a. hur länge lagringen ska ske, ett geografiskt definierat område, vilka personer som berörs, uppgiftskategorier, kommunikationsmedel och den personkrets som berörs (punkterna 106–111, 117–119).

Domstolen ansåg dessutom att förhandskontroll, att lagringen sker inom unionen, att en hög skydds- och säkerhetsnivå garanteras, att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut och att de berörda personerna informeras utgör förutsättning för att behöriga myndigheter ska kunna få tillgång till dessa uppgifter (punkterna 120–122).

Enligt artikel 54 i stadgan får ingen bestämmelse i stadgan tolkas som att den medför rätt att bedriva verksamhet eller utföra handlingar som syftar till att sätta ur spel någon av de rättigheter och friheter som erkänns i stadgan eller att inskränka dem i större utsträckning än vad

som medges i stadgan. Formuleringen i artikel 54 i stadgan har många likheter med artikel 17 i Europakonventionen.

2.3.2 Lagstiftningen i utlandet

För den internationella jämförelsen utvaldes Sverige, Norge, Danmark och Tyskland samt Nederländerna och Schweiz. Det var en självklarhet att ta med de nordiska länderna i jämförelsen eftersom ländernas rättssystem och rättskultur liknar varandra. Även Tysklands rättssystem liknar Finlands system. Särskilt Tysklands lagstiftning har fått erkänsla i Europadomstolens avgöranden som har gällt Tyskland. I och med att Tyskland valts som jämförelseland har det framhävts att denna proposition är förenlig med de mänskliga rättigheterna.

Samtidigt med beredningen av underrättelselagstiftningen i Finland har Schweiz och Nederländerna påbörjat projekt i syfte att se över sin underrättelselagstiftning. Eftersom det är fråga om europeiska länder där rättsstatsprincipen är starkt förankrad kunde man utifrån dessa projekt även bedöma vilken praxis som utgör en god grund för denna regeringsproposition. Den reform av underrättelselagstiftningen som pågår i Norge har också aktivt följts upp.

2.3.2.1 Sverige

Militär underrättelseinhämtning bedrivs av Militära Underrättelse- och Säkerhetstjänsten, MUST, Försvarets radioanstalt, FRA, Försvarets materielverk, FMV, och Totalförsvarets forskningsinstitut, FOI.

Om försvarsförvaltningens underrättelseverksamhet föreskrivs genom en allmän lag om försvarsunderrättelseverksamhet och en förordning om försvarsunderrättelseverksamhet som kompletterar lagen. Den allmänna lagen kompletteras av speciallagar såsom lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, lagen om kvalificerade skyddsidentiteter och lagen om elektronisk kommunikation.

*Styrning*

Försvarsunderrättelseverksamhetens inriktning bestäms av Sveriges regering enligt lagen om försvarsunderrättelseverksamhet. De myndigheter som regeringen bestämmer får inom ramen för den allmänna inriktning som regeringen beslutar om ange en närmare inriktning av underrättelseverksamheten. I lagstiftningen har regeringen dessutom getts en möjlighet att utfärda preciserande förordningar.

Vid försvarsdepartementet finns ett samordningssekretariat för säkerhetspolitiska underrättelsefrågor (SUND) som ansvarar för beredning och samordning av frågor som gäller försvarsunderrättelseverksamhet på regeringskanslinivå. Myndigheterna för försvarsunderrättelseverksamhet samarbetar också för att samordna den underrättelseverksamhet som gäller objekt som är av intresse för både den civila och den militära underrättelsen.

*Underrättelsetjänstens uppgift*

I 1 § i försvarsunderrättelselagen har verksamhetsområdet för underrättelsen avgränsats så att underrättelseverksamhet bedrivs till stöd för svensk utrikes-, säkerhets- och försvarspolitik och för att kartlägga yttre hot mot Sverige. Med verksamheten stöds också svenskt deltagande i internationellt säkerhetssamarbete. Underrättelseverksamheten får endast avse utländska för-

hållanden. De bestämmelser som gäller teknisk underrättelse har utfärdats i lagen om signalspaning i försvarsunderrättelseverksamhet.

*Informationsinhämtningsmetoder och hur beslut fattas om dem*

Underrättelsemyndigheterna får i sin verksamhet använda teknisk och personbaserad underrättelseinhämtning (2 § i lagen om försvarsunderrättelseverksamhet). I fråga om teknisk inhämtning gäller den centrala befogenheten signalspaning, som regleras av en helhet bestående av flera lagar. Allmän lag är lagen om signalspaning i försvarsunderrättelseverksamhet, och den preciseras av förordningen om signalspaning i försvarsunderrättelseverksamhet. Helheten kompletteras av lagen om Försvarsunderrättelsedomstol och lagen om behandling av personuppgifter i signalspaningsverksamhet. (Lag om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet).

I Sverige fullgörs underrättelseverksamheten genom inhämtning, bearbetning och analysering av information. Informationen rapporteras till berörda myndigheter.

Bestämmelser om signalspaning finns i speciallagar och en specialförordning om detta. FRA har till uppgift att inhämta underrättelseinformation i enlighet med sina uppdrag och ställa den inhämtade informationen till uppdragsgivarnas förfogande. För att signalspaning ska kunna inledas förutsätts alltid ett uppdrag, som FRA enligt 4 § i signalspaningslagen kan ges av regeringen, Regeringskansliet, Försvarsmakten, Polismyndigheten eller Säkerhetspolisen.

Enligt signalspaningslagen avses med signalspaning inhämtning av signaler i elektronisk form. Definitionen är teknikneutral och täcker alla metoder för signalspaning, såsom t.ex. tråd- och radiosignalspaning samt manuell och automatiserad informationsinhämtning. Signalspaning fördelar sig över fyra faser, som är inriktning av signalspaningen, inhämtning av information, bearbetning och analys av informationen samt rapportering om informationen.

En förutsättning för att signalspaning ska få användas är att de förutsättningar som definieras både i försvarsunderrättelselagen och i den speciallag som gäller signalspaning uppfylls. Enligt försvarsunderrättelselagen ska det vara fråga om ett underrättelseuppdrag som stöder svensk utrikes-, säkerhets- och försvarspolitik och som gäller utländska förhållanden och i detta uppdrag kartläggs yttre hot mot Sverige. En signal får inte inhämtas, om både mottagaren och avsändaren befinner sig i Sverige. Spaning på kommunikation i tråd får endast bedrivas när kommunikationen överskrider Sveriges gräns.

I 1 § i den speciallag som gäller signalspaning definieras uttömmande de objekt som får kartläggas genom signalspaning:

-yttre militära hot mot Sverige,

-förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,

-strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,

-utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,

-allvarliga yttre hot mot samhällets infrastrukturer,

-konflikter utomlands med konsekvenser för internationell säkerhet,

-främmande underrättelseverksamhet mot svenska intressen, eller

-främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

Om det är nödvändigt med tanke på verksamheten, kan information också inhämtas för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt för att utveckla den teknik och metodik som behövs för informationsinhämtning på det verksamhetsområde som avses i försvarsunderrättelselagen.

Signalspaning förutsätter alltid tillstånd av Försvarsunderrättelsedomstolen som är en specialdomstol. En tillståndsansökan som gäller spaning i tråd bör innehålla en beskrivning av datainsamlingsuppgiften, information om vilken signalbärare man vill inrikta informationsinhämtningen på, de sökbegrepp som ska användas, hur länge tillståndet bör vara i kraft och andra omständigheter som signalspaningsmyndigheten vill åberopa. I lagen har också ställts exakta förutsättningar för när domstolen kan bevilja tillstånd och vad som bör framgå av tillståndet. Förutsättningarna för beviljande anknyter särskilt till verksamhetens och uppdragets lagenlighet och proportionalitet. Tillståndet får vara i kraft högst sex månader och det kan förnyas för högst sex månader i taget. Vid domstol tillvaratas medborgarnas integritet av särskilda integritetsskyddsombud som är eller har varit domare eller advokater.

Av tillståndet bör framgå informationsinhämtningsuppdraget, vilka signalbärare tillståndet gäller, vilka sökbegrepp eller kategorier av sökbegrepp som får användas, hur länge tillståndet är i kraft och andra villkor som behövs för att begränsa intrånget i en enskild persons integritetsskydd. Med sökbegrepp avses enligt förarbetet till lagen sådana begrepp med hjälp av vilka man kan söka igenom en informationsmängd och hitta de poster eller uppgiftskonstellationer där begreppet i fråga förekommer. Ett sökbegrepp kan också innehålla sådana variabler med vilka man kan avskilja större informationsmängder. Möjligheten att använda ett sökbegrepp som avser en enskild fysisk person har begränsats för att integritetsskyddet ska kunna säkerställas. Ett dylikt sökbegrepp kan endast användas, om det är särskilt viktigt för underrättelseverksamheten.

Informationsinhämtning i datakommunikationstrådar förutsätter samarbete med datakommunikationsoperatörerna. Lagen om elektronisk kommunikation förutsätter att de operatörer som äger tråd överför den kommunikation som överskrider Sveriges gränser till en eller flera fastställda accesspunkter. Vidare är operatörerna skyldiga att till myndigheten lämna sådan information som gör det enklare att ta hand om signalerna och hantera datatrafiken. Operatörerna ska vidta de ovan nämnda åtgärderna på ett sådant sätt att deras skyldigheter som anknyter till sekretess inte äventyras.

I 7 § i signalspaningslagen ställs för FRA en skyldighet att förstöra uppgifterna i vissa fall. Upptagningar eller uppteckningar av uppgifter som inhämtats i enlighet med lagen ska förstöras omedelbart, om innehållet berör en viss fysisk person och har bedömts sakna betydelse för den verksamhet som avses i 1 §. Likaså har FRA skyldighet att förstöra informationen omedelbart, om den gäller en bikthemlighet, källskydd eller kommunikation mellan en advokat och en klient i ett straffrättsligt ärende.

I 11 a § i signalspaningslagen förutsätts att en fysisk person så snart som möjligt och senast en månad efter att försvarsunderrättelseuppdraget har avslutats ska underrättas om när och i vilket syfte underrättelseverksamhet har bedrivits, om inget annat följer av sekretessbestämmelserna. Beslutet om att underrätta personen fattas av FRA.

*Rapportering*

De myndigheter som bedriver underrättelseverksamhet är skyldiga att rapportera till försvarsdepartementet om verksamhetens allmänna inriktning, internationellt samarbete samt om den underrättelse som utförs med särskilda informationsinhämtningsmetoder, dvs. personbaserad inhämtning och signalspaning. Underrättelsemyndigheterna ska också årligen utarbeta en offentlig översikt av underrättelseverksamheten under det gångna året.

Vid utgången av kalenderåret lämnar myndigheterna till regeringen sin årsberättelse, som bl.a. innehåller uppgifter om verksamhetens resultat och förslag till budget för underrättelseverksamheten för nästa år.

*Samarbete med brottsbekämpningsmyndigheterna*

Underrättelsemyndigheterna har inga befogenheter gällande brottsbekämpande eller brottsförebyggande. Underrättelsen kan inte sköta sådana uppgifter som enligt lagen eller andra bestämmelser hör till polisens, Säkerhetspolisens eller andra lagövervakande myndigheters brottsbekämpande eller brottsförebyggande befogenheter.

De myndigheter som svarar för försvarsunderrättelseverksamheten får dock ge stöd till andra lagövervakande myndigheter i deras brottsbekämpande och brottsförebyggande verksamhet. I fråga om detta konstateras det i förarbetet till lagen att Säkerhetspolisen för närvarande i flera hänseenden fungerar som en underrättelsetjänst och inriktar sig på att inhämta information också om verksamhet utomlands som äventyrar Sveriges säkerhet. Inom ramen för denna sin uppgift måste Säkerhetspolisen kunna utnyttja kapaciteten till informationsinhämtning också hos de myndigheter som svarar för underrättelseverksamheten.

Den nationella operativa polismyndigheten och skyddspolisen kan styra signalspaningsmyndighetens verksamhet. Med stöd av den förordning som preciserar behandlingen av personuppgifter i FRA brottsbekämpningsmyndigheterna föreskrivs att vissa säkerhetsmyndigheter har möjlighet att få direkt tillgång till de delar av FRA:s databas som innehåller underrättelserapporter.

*Internationellt samarbete*

De myndigheter som bedriver försvarsunderrättelseverksamhet kan i enlighet med regeringens exaktare bestämmelser, under de förutsättningar som lagen ger, samarbeta med andra länder och internationella organisationer inom underrättelseverksamhetens område.

FRA får bedriva internationellt samarbete med andra länder och internationella organisationer i signalspaningsfrågor i anknytning till bekämpning av terrorism och gränsöverskridande grov brottslighet i enlighet med 1 § 2 mom. 3 punkten i signalspaningslagen. En förutsättning för samarbetet är att dess mål är att stöda Sveriges statsledning och nationella säkerhet. De uppgifter som myndigheten ger andra länder och internationella organisationer får inte skada svenska intressen.

Försvarets radioanstalt underrättar försvarsdepartementet om de frågor som gäller inledandet och fortgången av samarbetet. Medan verksamheten pågår ska försvarsdepartementet också underrättas om viktiga frågor som kommer upp i samarbetet.

Statens inspektion för försvarsunderrättelseverksamheten (SIUN) ansvarar för kontroll och granskning av underrättelseverksamheten. SIUN övervakar efterlevnaden av lagstiftningen, inriktningen av försvarsunderrättelseverksamheten och de metoder som används vid informationsinhämtning.

Endast SIUN, som är övervakande myndighet, har tillträde till den kommunikation som operatörerna överför till sina samverkanspunkter. SIUN har till uppgift att avskilja och till FRA överlåta endast de signalbärare som specificeras i domstolens tillstånd. De sökningar som FRA gör inriktas på dessa bärare. FRA rapporterar den information som inhämtats genom signalspaning till uppdragsgivaren samt med de förutsättningar som fastställs i lagen också till övriga myndigheter.

Den granskning som SIUN utför gäller enligt 10 § i signalspaningslagen framför allt användningen av sökbegrepp i signalspaningen, förstöring av uppgifter och rapportering. SIUN kan också bestämma att en spaningsåtgärd ska avslutas och uppgifterna förstöras, ifall verksamheten inte har stämt överens med tillståndet. SIUN kan på begäran av en fysisk person kontrollera, om dennes meddelanden har inhämtats och om den eventuella inhämtningen har varit förenlig med lagen.

Inom FRA finns Integritetsskyddsrådet, som har till uppgift att övervaka att integritetsskyddet realiseras. Rådet rapporterar till FRA:s ledning och vid behov till SIUN. Datainspektionen övervakar att integritetsskyddet realiseras också i FRA:s verksamhet. Om behandlingen av personuppgifter som inhämtats genom signalspaning föreskrivs i en särskild lag. Vidare övervakas signalspaningen av riksdagens justitieombudsman och justitiekanslern.

Den parlamentariska representationen vid granskningen av underrättelseinhämtningen förverkligas genom SIUN, vars medlemmar utnämns av regeringen. Partiernas riksdagsgrupper kan påverka sammansättningen av SIUN, som bildas av en ordförande, en vice ordförande och fem medlemmar. Regeringen utnämner medlemmarna bland de kandidater som partiernas riksdagsgrupper har ställt upp. För närvarande består SIUN av representanter för Socialdemokratiska arbetarepartiet, Moderata samlingspartiet och Liberalerna. Regeringen överlämnar årligen en skrivelse till riksdagen. I skrivelsen lämnar regeringen en redovisning för resultaten av uppföljningen och kontrollerna gällande inhämtning av försvarsunderrättelser inom signalspaningsverksamheten under det föregående året.

2.3.2.2. Norge

Norges underrättelsetjänst för utlandet är Etterretningstjenesten (E-tjenesten), vars uppgifter och befogenheter fastställs i lag och förordning (Lag om Etterreningstjenesten, Instruks om Etterretningstjenesten). I Norge finns ingen nationell säkerhetstjänst, utan för upprätthållandet av landets interna nationella säkerhet ansvarar 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 utgör en del av det norska försvaret. Försvarsmaktens kommendör är förman för underrättelsetjänstens chef. Chefen för underrättelsetjänsten fungerar som rådgivare för försvarsmaktens kommendör i ärenden som gäller underrättelseinhämtning.

Försvarsdepartementet har ansvaret för den politiska styrningen och övervakningen av verksamheten inom underrättelsetjänsten. Underrättelsetjänsten håller departementet informerat om sin verksamhet och får uppdrag av det. Styrningen, övervakningen och rapporteringen sker via försvarsmaktens kommendör.

Underrättelsetjänsten är förpliktad att föredra vissa viktiga ärenden för försvarsdepartementets beslutsfattande. Ärenden i vilka beslut ska fattas av departementet är inledning av samarbete med nya internationella parter, tillhandahållande av bemanningsberedskap, inledning av politiskt känsliga s.k. särskilda operationer för underrättelseinhämtning samt andra särskilt viktiga eller principiellt viktiga ärenden.

Övriga departement och myndigheter kan med försvarsdepartementets tillstånd ge uppdrag till underrättelsetjänsten.

*Underrättelsetjänstens uppgift*

En allmän uppgift för underrättelsetjänsten är att skaffa, bereda och analysera information som gäller Norges intressen i förhållande till främmande stater, organisationer och individer samt sammanställa hotbedömningar och bedömningar med avseende på underrättelseinhämtning för att trygga nationella intressen. I lagen ingår en förteckning över nationella intressen som ska tryggas. Det kan bl.a. handla om utformningen av den norska utrikes-, säkerhets- och försvarspolitiken, beredskapsplanering och utveckling av strukturerna inom försvarsmakten samt tillgången till information om internationell terrorism, gränsöverskridande miljöproblem och massförstörelsevapen. Förteckningen är inte uttömmande och de förändringar som sker i Norges säkerhetsmiljö är avgörande för vilka nationella intressen som underrättelsetjänsten tryggar vid en viss tidpunkt. Enligt den norska förordningen om underrättelsetjänsten är den huvudsakliga uppgiften dock informationsinhämtning om sådan politisk och samhällelig utveckling, planer och militär kapacitet i andra stater, som kan utgöra ett hot mot Norges säkerhet. Enligt förordningen hör stöd i form av underrättelseinhämtning till norska truppförband som deltar i internationella militära insatser till de prioriterade uppgifterna. Försvarsdepartementet beslutar om den inbördes prioriteringen av underrättelseuppdrag som gäller civila efter att ha förhandlat om saken med underrättelsetjänsten samt andra myndigheter som behöver underrättelseinformation.

*Informationsinhämtningsmetoder och hur beslut fattas om dem*

Det finns inga bestämmelser om underrättelsetjänstens informationsinhämtningsmetoder eller de metoder den använder för personbaserad underrättelseinhämtning och teknisk inhämtning. Den omständighet att underrättelsetjänsten överhuvudtaget kan använda sig av hemliga informationsinhämtningsmetoder framgår endast indirekt av lagstiftningen. Förordningen om underrättelsetjänsten kompletterades 2013 med bestämmelser om förutsättningarna för informationsinhämtning som inriktas på norska personer som vistas utomlands. Bestämmelserna i sig preciserar inte metoderna för informationsinhämtning utan de ställer begränsningar för i vilket syfte och under vilka betingelser information om norska medborgare som vistas utomlands kan inhämtas. Enligt de kompletterande bestämmelserna avses emellertid med informationsinhämtning övervakning och annan hemlig informationsinhämtning. Av den förordning som gäller samarbetet mellan underrättelsetjänsten och polisens säkerhetstjänst kan man även

sluta sig till att hemlig informationsinhämtning förekommer. Enligt förordningen ska parterna utbyta information om utvecklingen i fråga om teknologi och metoder samt ge varandra stöd i anslutning till utrustning och teknik under konkreta informationsinhämtningsoperationer. Det faktum att underrättelsetjänsten är skyldig att underställa ministeriet beslutsfattandet om politiskt känsliga särskilda underrättelseoperationer tyder också på att hemliga informationsinhämtningsmetoder tillämpas.

*Rapportering*

Underrättelsetjänsten är skyldig att hålla försvarsdepartementet samt andra departement som det beslutar om informerade om förändringar i Norges externa säkerhetspolitiska omgivning. Direkt uppgiftsrapportering till uppdragsgivare som står utanför försvarsförvaltningen kräver försvarsdepartementets tillstånd.

*Samarbete med brottsbekämpningsmyndigheterna*

Det finns inga konkreta bestämmelser om utlämnande av underrättelsetjänstens uppgifter i syfte att förebygga, avslöja eller utreda brott. Det finns dock en egen förordning som gäller samarbetet mellan underrättelsetjänsten och polisens säkerhetstjänst. Polisens säkerhetstjänst har till uppgift att förebygga, avslöja och utreda vissa brott som riktas mot den nationella säkerheten.

När det gäller informationsutbyte mellan parterna och annat samarbete är bekämpning av terrorism, spridning av massförstörelsevapen och olaglig underrättelseverksamhet samt övriga omständigheter som gäller intressen som är viktiga för Norge prioriterade områden enligt förordningen. Parterna ska bistå varandra såväl i fråga om konkreta operationer för informationsinhämtning och utbyte av operativ information som analysering av strategisk information och hotbedömning. Samarbetet kan även ta sig uttryck i form av tekniskt stöd och utbildningsstöd till varandra, tjänstemannautbyte och internationell kontaktpersonsverksamhet. En förutsättning för samarbetet är att parterna iakttar de bestämmelser som gäller för deras egna befogenheter. Normalt fattas besluten om begäran om och givande av stöd i anslutning till genomförandet av operationer för informationsinhämtning av cheferna för dessa tjänster. I särskilt viktiga frågor är det dock departementen som styr tjänsternas verksamhet.

Förordningen angående samarbete förpliktar parterna att utbyta s.k. överskottsinformation. Med överskottsinformation avses sådan information som tjänsten har fått tillgång till i samband med sin informationsinhämtning men som inte hör till dess verksamhetsområde. Överskottsinformation kan gälla personuppgifter exempelvis i fråga om personer som vistas utomlands och som äventyrar Norges intressen. En part som har lämnat ut överskottsinformation kan förutsätta att mottagaren inte ger informationen vidare utan utlämnarens tillstånd. Enligt förordningen om underrättelsetjänsten får underrättelsetjänsten lämna ut överskottsinformation som gäller personuppgifter som den fått i samband med informationsinhämtning även till andra norska myndigheter än polisens säkerhetstjänst.

Underrättelsetjänsten får inte utsätta norska medborgare eller norska juridiska personer för hemlig informationsinhämtning på norsk mark. Som ett undantag från det här kan underrättelsetjänsten dock inrikta hemlig informationsinhämtning på sådana norska personer som vistas i Norge och som deltar i olaglig underrättelseverksamhet för en främmande stat. Underrättelsetjänstens informationsinhämtning ska då ske genom förmedling av polisens säkerhetstjänst eller med dess godkännande.

Det finns inga bestämmelser om samarbetet mellan underrättelsetjänsten och den öppna polisen. Av förordningen angående samarbete framgår emellertid indirekt att ett samarbete existerar, eftersom det framgår av tillämpningsbestämmelsen att förordningen inte ska tillämpas på sådant stöd eller sådana utlämnanden av information som underrättelsetjänsten ger tullmyndigheterna eller den öppna polisen. Enligt förordningen kan den här typen av utlämnanden emellertid kanaliseras via polisens säkerhetstjänst. Underrättelsetjänsten kan genom förmedling av polisens säkerhetstjänst ställa villkor för hur den polisenhet som är slutlig mottagare av uppgifterna får använda uppgifterna samt kräva att polisens säkerhetstjänst inte avslöjar att uppgifterna kommer från underrättelsetjänsten.

*Internationellt samarbete*

Enligt lagen om underrättelsetjänster får underrättelsetjänsten inleda samarbete i fråga om underrättelseinhämtning och bedriva sådant samarbete med främmande makter. Försvarsdepartementet beslutar om upprättandet av samarbetsförbindelser på förslag av underrättelsetjänsten. Underrättelsetjänsten och polisens säkerhetstjänst är förpliktade att samordna sina internationella samarbetsförbindelser.

År 2013 togs in i förordningen om underrättelsetjänster kompletterande bestämmelser om de förutsättningar på vilka underrättelsetjänsten får lämna ut personuppgifter om norska medborgare till utländska underrättelsetjänster. Informationen får utlämnas om det här är förenligt med de uppgifter som fastslagits för underrättelsetjänsten och underrättelsetjänsten har rätt att lagra den i sitt personregister. Dessutom förutsätts att utlämnandet sker i enlighet med Norges intressen, att det bedöms vara nödvändigt då man överväger tryggandet av sinsemellan viktiga nationella intressen och följderna för den person som uppgifterna gäller och att ett utlämnande är försvarbart med beaktande av uppgifternas art, den person som uppgifterna gäller samt den instans som är mottagare av uppgifterna. I samband med utlämnandet ska ställas ett villkor att informationen inte får användas som grund för hemlig informationsinhämtning, som riktas mot personer som vistas på norsk mark. Ovan nämnda förutsättningar är endast tillämpliga då det är fråga om utlämnande av norska medborgares personuppgifter. Det ställs inga villkor för utlämnandet av utländska personers personuppgifter.

*Ett lagstiftningsprojekt som gäller underrättelseinhämtning som avser datatrafik*

Norges försvarsminister tillsatte i februari 2016 en kommitté för att utvärdera behovet av bestämmelser om underrättelseinhämtning som avser datatrafik. Kommittén överlämnade sitt betänkande (Digitalt grenseforsvar (DGF). Lysne II-utvaget. (26.08.2016)) till försvarsministern i september 2016.

I sitt betänkande föreslog kommittén lagstiftning om underrättelseinhämtning som avser datatrafik eftersom den ansåg att det är fråga om nödvändiga befogenheter för att skydda det demokratiska samhället och den nationella säkerheten. Enligt kommittén ska befogenheterna tilldelas E-tjenesten och de ska kunna användas för informationsinhämtning bl.a. i fråga om allvarliga cyberhot, terrorism och spionerі riktat mot Norge. Användningssyftet ska hänföras till E-tjenestens uppgifter och det ska också motsvara de prioriteringar för underrättelseverksamheten som regeringen årligen anvisar för tjänsten. Prioriteringarna för underrättelseverksamheten är inte offentliga och det är således inte känt om den föreslagna informationsinhämtningen till sin natur grundar sig på hot eller är mer omfattande.

I fråga om sådan underrättelseinhämtning som avser datatrafik som kommittén föreslår skulle det vara fråga om att med hjälp av sökbegrepp filtrera datatrafiken i datakommunikationstrå-

dar som överskrider den norska gränsen. Inom verksamheten skulle det vara tillåtet att tillämpa både sökbegrepp som beskriver innehållet och andra sökbegrepp, men det kräver förhandsgodkännande av domstol. Enligt kommitténs ståndpunkt måste den eventuella överskottsinformation som fås inom verksamheten utplånas i alla situationer. Man får således endast lagra sådan information, som direkt anknyter till E-tjenestens uppgifter och de prioriteringar för underrättelseverksamheten som regeringen anvisar E-tjenesten. Kommittén tog inte ställning till utlämnande av den här typen av uppgifter till polismyndigheterna men konstaterade att uppgifter från underrättelseinhämtning som avser datatrafik under inga omständigheter bör få användas som bevis i rättegång.

Kommittén anser att sådan underrättelseinhämtning som avser datatrafik som regleras tillräckligt exakt på lagnivå skulle bidra till att förbättra verksamhetsbetingelserna för det norska näringslivet. Kommittén avvisade åsikterna om att Norge som en ”underrättelsefri zon” skulle ha en tilldragande effekt när det gäller internationella investeringar. En tillräckligt avgränsad och transparent lagstiftning i kombination med underrättelsemyndigheternas förbättrade förmåga att avvärja cyberhot mot Norge skulle tvärtom stärka Norges internationella konkurrenskraft och göra landet mer attraktivt som ett investeringsobjekt.

Kommittén ansåg också att man kan reglera om underrättelseinhämtning som avser datatrafik på ett sätt som harmonierar med Norges internationella förpliktelser som gäller de mänskliga rättigheterna, som följer av Europeiska konventionen om mänskliga rättigheter (EIS), samt tolkningspraxis inom EU-rätten. Det här förutsätter att en eventuell lag om underrättelseinhämtning som avser datatrafik innehåller tillräckligt tydliga bestämmelser om användningsändamålen för underrättelseinhämtning som avser datatrafik och hanteringen av de uppgifter som inhämtningen resulterar i samt rättsskyddsmekanismer. Kommittén föreslog att de rättsskyddsarrangemang som bör kopplas samman med underrättelseinhämtning som avser datatrafik ska vara såväl preventiva som utförbara i efterhand. Det preventiva rättsskyddet ska genomföras genom bestämmelser om att besluten om underrättelseinhämtning som avser datatrafik ska fattas av domstol. Det förutsätts att domstolen ska godkänna användningen av sökbegrepp som beskriver innehållet i meddelanden som används vid filtrering. Den metadata som insamlas vid underrättelseinhämtning som avser datatrafik ska lagras i ett datalager som skapas för ändamålet och de sökningar som inriktas på datalagret ska också godkännas av domstol. Enligt kommittén vore det önskvärt att domstolen är insatt i den verksamhetsmiljö som omfattar underrättelseinhämtning, E-tjenestens verksamhet och tekniska frågor. Domstolens medlemsantal ska vara begränsat av konfidentiella skäl. Det här kan utgöra en motivering till att det inrättas en specialdomstol.

Enligt kommitténs bedömning behövs det både en förstärkning av laglighetskontrollerna och delvis även en förstärkning av den parlamentariska övervakningen för att rättsskyddet ska kunna garanteras i efterhand. Enligt kommittén bör det för laglighetskontroll av underrättelseinhämtning som avser datatrafik inrättas ett nytt organ ("DGF-tilsynet"), som bör få information bl.a. om alla sökningar som utförts i metadatalagret, de tillstånd som domstolen har beviljat för underrättelseinhämtning som avser datatrafik och deras verkställighet samt om konfigurering av filter som används vid underrättelseinhämtning som avser datatrafik. EOS-delegationen som enligt vad som ovan konstaterats inte kan anses som ett rent parlamentariskt kontrollorgan föreslås övervaka underrättelseinhämtning som avser datatrafik på samma sätt som E-tjenestens verksamhet i övrigt. Det föreslås att DGF-tilsynet förpliktas att lämna in rapporter till delegationen och ska få begränsad tillgång till informationssystem som gäller underrättelseinhämtning som avser datatrafik. EOS-delegationen ska rapportera till norska stortinget om hur underrättelseinhämtning som avser datatrafik används och även om försvarsdepartementets styrning av delegationen.

Betänkandet innehåller en detaljerad analys av EU-domstolens rättsfall under den senaste tiden. Den underrättelseinhämtning som avser datatrafik som ordnats enligt ovan beskrivna riktlinjer bedöms vara förenlig med de rättsnormer som ingår i de avgöranden som getts med anledning av ärendena Digital Rights m.fl (C-293/12) och Schrems (C-362/14) som även behandlas i det här betänkandet. Avgörandena anses även i övrigt endast delvis vara tillämpliga på underrättelseinhämtning som avser datatrafik.

Betänkandet innehåller också en internationell jämförelse som är mer omfattande även om den är mer generell än den som ingår i denna proposition. Stater som man kan jämföra med är Sverige, Frankrike, Storbritannien, Canada, Tyskland, Nederländerna, Schweiz och Finland. Kommittén konstaterar tydligt att den utgår från att även många sådana länder som saknar bestämmelser om underrättelseinhämtning som avser datatrafik använder sådan underrättelseinhämtning trots att rättsgrunden är bristfällig. Kommittén anser att såväl beaktandet av de grundläggande och mänskliga rättigheterna som omständigheter som anknyter till oförutsägbarhet när det gäller ekonomiska förhållanden talar för en öppen och exakt reglering i frågan.

Av betänkandet framgår att den nationella säkerhetsmyndigheten i Norge administrerar det nationella systemet för observationer av datasäkerhetsintrång som grundar sig på filtrering. Av den beskrivning av systemet för observationer som ingår i betänkandet kan man dra den slutsatsen att det i fråga om riktlinjerna motsvarar Kommunikationsverkets s.k. HAVARO-system som tas upp senare i betänkandet. Enligt betänkandet är systemet för observationer inte tillräckligt bra för att upptäcka de allvarligaste cyberhoten mot Norge och därför är det nödvändigt att reglera om underrättelseinhämtning som avser datatrafik för att skydda sig mot sådana hot.

I Norge har inletts ett projekt som syftar till att utifrån betänkandet förnya lagstiftningen om underrättelseinhämtning.

2.3.2.3 Danmark

I Danmark ansvarar försvarsmaktens underrättelsetjänst Forsvarets Efterretningstjeneste FE, för utrikes underrättelseinhämtning. Bestämmelser om dess uppgifter, befogenheter och övervakningen av verksamheten ingår i Loven om Forsvarets Efterretningstjeneste. Danmark har ingen nationell säkerhetstjänst utan för upprätthållandet av den interna nationella säkerheten ansvarar säkerhetspolisen, Politiets Efterretningstjeneste, PET, som har befogenheter i fråga om brottsbekämpning.

*Styrning*

Försvarsmaktens underrättelsetjänst hör trots namnet inte till försvarsmakten utan är en civil myndighet som lyder under och styrs av danska försvarsministeriet. Försvarsministern kan anvisa underrättelsetjänsten uppgifter som anknyter till dess verksamhetsområde som definieras i lag.

*Underrättelsetjänstens uppgift*

FE:s uppgifter enligt lag är att skapa en underrättelsemässig grund för den danska utrikes-, säkerhets- och försvarspolitiken, hjälpa att förebygga och avvärja hot som riktas mot Danmark och danska intressen och att i dessa syften insamla, analysera och rapportera sådan information om utländska förhållanden som är av betydelse för Danmark och danska intressen utom-

lands. FE är även s.k. nationell säkerhetsmyndighet och nationell datasäkerhetsmyndighet i Danmark.

*Informationsinhämtningsmetoder och hur beslut fattas om dem*

Det finns ingen egentlig reglering om de konkreta informationsinhämtningsmetoder som underrättelsetjänsten använder eller om förutsättningarna för användningen av dem. Enligt lagen om försvarsmaktens underrättelsetjänst får FE samla in och skaffa information som kan vara av betydelse för dess underrättelsetjänst. Enligt förarbetena till lagen har gränsen för informationsinhämtning medvetet ställts mycket lågt. Enligt förarbetena är en av underrättelsetjänstens synnerligen viktiga uppgifter att upptäcka nya okända hot mot säkerheten. I sådana fall kan föremålet för informationsinhämtningen inte specificeras i det skede då den inleds. Avsikten var enligt förarbetena att bestämmelsen om informationsinhämtning skulle skrivas så att den medger inhämtning av synnerligen stora informationsmassor.

I lagen särskiljs inte underrättelsetjänstens metoder för underrättelseinhämtning. Enligt offentliga källor utförs informationsinhämtning såväl genom inhämtning av personuppgifter, med hjälp av signalspaning elektroniskt från satelliter och spaning på datakommunikation i tråd som genom öppna källor.

Liksom i Norge har man även i Danmark nyligen särskilt reglerat om de förutsättningar med stöd av vilka man får inrikta informationsinhämtning på egna medborgare som är bosatta utomlands. Informationsinhämtning får inriktas på danska fysiska personer och juridiska personer som befinner sig utomlands, om det finns grundad anledning att befara att den som är föremål för informationsinhämtning deltar i verksamhet som föranleder terrorismhot mot Danmark eller danska intressen. Om informationsinhämtningen förutsätter att man ingriper i skyddet för förtroliga meddelanden ska tillstånd ansökas hos domstol. Ansökan ska innehålla uppgifter om personen eller de personer som informationsinhämtningen gäller samt om de omständigheter med stöd av vilka de med grundad anledning kan antas ta del av verksamhet som föranleder terrorismhot mot Danmark eller danska intressen.

Tillståndsförfarandet tillämpas endast på sådana fall där det är nödvändigt att inrikta informationsinhämtning på en dansk medborgare. Att ingripa i utländska fysiska eller juridiska personers konfidentiella kommunikation kräver inget tillstånd av domstol.

*Rapportering*

Underrättelsetjänsten är förpliktad att kontinuerligt underrätta försvarsministeriet om sådana händelser och utveckling inom tjänstens verksamhetsområde som påverkar Danmark och danska intressen samt om omständigheter som i betydande omfattning påverkar underrättelsetjänstens egen verksamhet. Dessutom ska underrättelsetjänsten informera ministeriet om de mest betydande enskilda ärenden som den har hanterat. Det finns ingen reglering om övrig rapportering.

*Samarbete med brottsbekämpningsmyndigheterna*

Polisens säkerhetstjänst PET ansvarar för förebyggande, avslöjande och utredning av brott som äventyrar den nationella säkerheten, bl.a. terroristbrott samt högförräderibrott och landsförräderibrott.

Underrättelsetjänsten och polisens säkerhetstjänst får till varandra lämna ut personuppgifter och annan information, om utlämnandet kan ha betydelse för någondera partens fullgörande av sina uppgifter. Syftet är att parterna inte särskilt ska behöva bedöma om utlämnandet är nödvändigt i samband med varje enskilt utlämnande av information. Enligt ett statligt betänkande där det föreslås lagstiftning om FE och PET är tjänsternas uppgifter så starkt knutna till varandra att överlåtelse av information mellan dem långt kan jämföras med en myndighets interna informationsöverlåtelser.

Underrättelsetjänsten får lämna ut uppgifter som gäller danska medborgare till andra polisenheter än polisens säkerhetstjänst, om utlämnandet kan ha betydelse för underrättelsetjänsten med avseende på hur den sköter sina fastställda uppgifter. Under samma förutsättningar får den lämna ut sådan information även till andra myndigheter i hemlandet.

*Internationellt samarbete*

Lagen innehåller inga bestämmelser om underrättelsetjänstens internationella samarbete. Av lagens förarbeten framgår att eftersom Danmark är ett litet land är det helt beroende av utländska parters uppgifter och därför måste underrättelsetjänsten bedriva intensivt operativt samarbete med säkerhets- och underrättelsetjänster i andra stater. Underrättelsetjänstens rätt att lämna ut information som gäller danska medborgare till andra stater och internationella organisationer har begränsats så att utlämnandet ska vara av betydelse för underrättelsetjänstens skötsel av sina lagstadgade uppgifter. Information kan således lämnas ut till utlandet under samma förutsättningar som till de nationella myndigheterna.

2.3.2.4 Tyskland

Bundesnachrichtendienst (BND) är Tysklands underrättelsetjänst för utlandet och ansvarar för extern informationsinhämtning gällande såväl civila som militära hot. Uppgifterna för Tysklands nationella säkerhetstjänst fördelas så att förbundsstatens civila säkerhetstjänst är Bundesverfassungsschutz (BfV) och militära säkerhetstjänst Militärischer Abschirmsdienst (MAD). Bestämmelser om uppgifterna och befogenheterna för alla ovan nämnda aktörer ingår i egna lagar även om de lagar som gäller BND:s och MAD:s verksamhet i fråga om befogenheterna i stor utsträckning hänvisar till den lag som gäller BfV:s verksamhet. Med tanke på befogenhetsregleringen är även den lag av stor betydelse som begränsar post- och telehemligheten (G10-lagen; Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses). Lagen innehåller bestämmelser om alla de underrättelseinhämtningsmetoder genom vilka säkerhets- och underrättelsetjänstens informationsinhämtning kan ingripa i skyddet för förtroliga meddelanden.

Tyskland är en förbundsstat där förbundsstaten och delstaterna har delad befogenhet i ärenden med anknytning till inrikes frågor. Av det här följer att utöver förbundsstatens civila säkerhetstjänst BfV finns en egen civilsäkerhetstjänst (Landesverfassungsschutz) i varje delstat. Eftersom utrikes- och försvarsärendena hör till förbundsstatens exklusiva befogenhet, saknar delstaterna egna underrättelsetjänster för utlandet eller militära säkerhetstjänster.

*Styrning*

Tysklands underrättelsetjänst för utlandet BND lyder under och styrs av förbundskanslersämbetet. För styrningen ansvarar en koordinator av underrättelseinhämtningen vid förbundskanslersämbetets stab. Förbundsstatens civila säkerhetstjänst BfV lyder på motsvarande sätt under och styrs av förbundsstatens inrikesministerium och den militära säkerhetstjänsten MAD un-

der förbundsstatens försvarsministerium. Delstaternas säkerhetstjänster är inte underställda förbundsstatens säkerhetstjänst utan de lyder under inrikesministeriet i respektive delstat. Eftersom befogenheterna är uppdelade finns det särskilda bestämmelser om samarbetet mellan förbundsstatens säkerhetstjänst och delstaternas säkerhetstjänster.

Det finns inga närmare bestämmelser i lag om användningen av ministeriernas styrningsbefogenheter. Det finns inga bestämmelser i lag om förutsättningarna och beslutsprocesserna för användning av andra hemliga metoder för informationsinhämtning än sådana som ingriper i skyddet för förtroliga meddelanden. Sådana bestämmelser ingår i underrättelse- och säkerhetstjänsternas reglementen, som utfärdas av de ministerier som ansvarar för verksamheten. Utfärdandet av reglementen, som är sekretessbelagda, kan redan i sig anses som en viktig form av styrningsbefogenheter. Man torde dessutom kunna anta att reglementena innehåller närmare föreskrifter om den konkreta styrningen av säkerhets- och underrättelsetjänsterna.

En form av styrning som är värd att beakta är att de ministerier som ansvarar för verksamheten vid säkerhets- och underrättelsetjänsterna deltar i beslutsfattande som gäller användning av hemliga metoder för informationsinhämtning som ingriper i skyddet för förtroliga meddelanden. Det styrande ministeriet godkänner i förhand exempelvis ansökningar som gäller teleavlyssning och underrättelseinhämtning som avser datatrafik innan de, beroende av informationsinhämtningsmetod, överförs till tillståndsförfarandet hos myndigheten för laglighetskontroll eller den parlamentariska tillsynsmyndigheten.

*Underrättelsetjänstens uppgift*

I lag föreskrivs att BND har till uppgift att inhämta och analysera underrättelseinformation som är av betydelse för Tysklands utrikes- och säkerhetpolitik. En allmän förutsättning för inhämtning av information angående händelser utomlands som har utrikes- och säkerhetspolitisk betydelse är att den inte kan inhämtas på något annat sätt och att ingen annan myndighet ansvarar för inhämtningen.

Det är en lagstadgad uppgift för BfV och delstaterna att inhämta och analysera underrättelseinformation om sådan verksamhet som strider mot den demokratiska samhällsordningen och den konstitutionella ordningen liksom även verksamhet som äventyrar förbundsstatens och delstaternas existens och säkerhet. De ska dessutom inhämta och analysera information om underrättelseverksamhet för främmande staters räkning och annan verksamhet som undergräver grunden för Tysklands säkerhet, våldsbetonade avsikter som äventyrar Tysklands yttre säkerhetsintressen samt initiativ som strider mot internationellt samförstånd eller en fredlig samexistens mellan folk. Sammanslutningar som främjar sådana här initiativ är förbjudna enligt den grundlag som stiftades i Tyskland efter andra världskrigets slut.

Den militära säkerhetstjänsten MAD inhämtar och analyserar underrättelseinformation om liknande hot som BfV men dock under förutsättning att hoten i fråga riktas mot personalen, enheterna eller inrättningarna inom försvarsministeriets förvaltningsområde och att det är en arbetstagare inom försvarsministeriets förvaltningsområde som står bakom hoten. Dessutom ska MAD inhämta och analysera information om eventuella fall där personalen inom försvarsministeriets förvaltningsområde deltar i initiativ som strider mot internationellt samförstånd eller en fredlig samexistens mellan folk. MAD:s främsta uppgift är således att upptäcka och avvärja sådana hot som väller fram inom Tysklands försvarsförvaltning. Dessutom ska MAD bedöma säkerheten för de enheter och baser som lyder under försvarsförvaltningen och även för de Nato-baser som är placerade i Tyskland oavsett vilken aktörs verksamhet som

eventuellt äventyrar dessa. Till den sistnämnda uppgiften anknyter inga egna befogenheter för informationsinhämtning utan det gäller att analysera uppgifter som fås från andra parter.

*Informationsinhämtningsmetoder och hur beslut fattas om dem*

Tysk lagstiftning delar in underrättelse- och säkerhetstjänsternas hemliga metoder för underrättelseinhämtning i sådana där man inte gör intrång i innehållet i förtroliga meddelanden som åtnjuter särskilt skydd enligt tysk grundlag, och sådana där man gör intrång i innehåll av detta slag. Bestämmelser om s.k. allmänna metoder för underrättelseinhämtning, som tillhör den förra gruppen ingår i speciallagar om underrättelse- och säkerhetstjänsternas verksamhet samt i de reglementen som de styrande ministerierna har utfärdat i fråga om tjänster som lyder under dem. Bestämmelser om metoder för underrättelseinhämtning som tillhör den senare gruppen, dvs. metoder som gör intrång i innehållet i förtroliga meddelanden, ingår gemensamt för alla tjänster i den s.k. G10-lagen.

I 8 § i BfV-lagen ingår en grundläggande bestämmelse som gäller användningen av allmänna metoder för underrättelseinhämtning. Enligt bestämmelsen kan säkerhetstjänsten utnyttja sådana hemliga metoder för informationsinhämtning, exempelvis användning och styrning av informationskällor, infiltration, optisk observation, teknisk avlyssning, falska handlingar och registreringsskyltar, om nödvändig information inte går att få genom mindre ingrepp i integriteten. Den förteckning som ingår i bestämmelsen innehåller exempel på hemliga metoder för informationsinhämtning. Mer konkret föreskrivs om informationsinhämtningsmetoder samt om förutsättningarna för användning av dem och beslutsfattande gällande användningen i BfV-reglementet, som godkänns av förbundsstatens inrikesminister och delges det parlamentariska kontrollorganet. BfV-reglementet är ingen offentlig handling.

I 8 a § och 9 § i BfV-lagen ingår vissa särskilda bestämmelser om säkerhetstjänstens rätt att få information och tekniska informationsinhämtningsmetoder. Den förstnämnda bestämmelsen gäller BfV:s rätt att få tillgång till kunduppgifter från flygbolag, banker och andra finansinstitut, företag som tillhandahåller posttjänster samt sådana som tillhandahåller teletjänster utan hinder av sekretessbestämmelser. Även s.k. retroaktiva teleövervakningsuppgifter omfattas av rätten att få information. För begäran om uppgifter av post- och teleföretag krävs ett beslut av chefen för BfV eller hans eller hennes ställföreträdare. Beslut som gäller begäran om passagerar- samt 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 då det är nödvändigt för att avvärja överhängande fara och då polisen inte kan vidta åtgärder i tid. Beslut om avlyssning eller observation av en bostad fattas av chefen för säkerhetstjänsten eller hans eller hennes ställföreträdare och fastställs av tingsrätten. Bestämmelser om lokalisering av mobiltelefoner ingår även i 9 § i BfV-lagen.

Bestämmelserna i lagarna angående BND:s och MAD:s verksamhet om allmänna metoder för underrättelseinhämtning hänvisar till de bestämmelser i BfV-lagen som redogörs för ovan. BND har rätt att inom sitt eget verksamhetsområde använda sådana metoder för underrättelseinhämtning som avses i 8, 8a och 9 § i BfV-lagen och sådana som föreskrivs närmare i dess eget reglemente. MAD har samma rätt inom sitt eget verksamhetsområde, men den är avsevärt snävare.

Enligt 10 § i den tyska grundlagen är skyddet för förtroliga meddelanden okränkbart och kan begränsas endast genom lag. Därför har bestämmelserna om metoder för underrättelseinhämtning som riktas mot innehållet i förtroliga meddelanden samlats i en egen speciallag, G10-lagen, som utgör grunden för befogenheterna för alla tjänster.

I G10-lagen fastställs de förutsättningar på vilka säkerhets- och underrättelsetjänsterna får kontrollera förtroliga meddelanden som förmedlas av posten och avlyssna samt spela in förtrolig telekommunikation. För att få utnyttja dessa befogenheter krävs ett skriftligt tillstånd av det ministerium som ansvarar för verksamheten och ett skriftligt förhandsgodkännande av organet för laglighetskontroll (den s.k. G10-kommissionen). Nationella säkerhetstjänster får kontrollera postförsändelser och utföra teleavlyssning endast om det med fog kan antas att en person planerar att utföra ett visst brott eller har utfört ett visst brott. Lagen innehåller en synnerligen omfattande förteckning över brott om vilka information kan inhämtas med stöd av befogenheterna. Ett gemensamt drag för dessa brott är att de kan anses rikta sig mot den nationella säkerheten. De nationella säkerhetstjänsterna kan använda befogenheterna i fråga även om en person med fog kan antas vara medlem av en sådan sammanslutning, vars syfte är att utföra brott mot den nationella säkerheten. Utöver den förmodade gärningsmannen kan befogenheterna även användas i fråga om personer som rimligen kan antas ha kontakt med honom eller henne. Befogenheterna får användas endast då inhämtning av information med hjälp av andra metoder är omöjligt eller avsevärt svårare. Det är inte tillåtet att med hjälp av öppnande av postförsändelser eller teleavlyssning inhämta information om sådana omständigheter som en person med stöd av straffprocesslagen har rätt att vägra vittna om. Även det s.k. kärnområdet i privatlivet omfattas av ett utvidgat skydd mot myndigheternas informationsinhämtning. Om det finns anledning att anta att en åtgärd endast resulterar i information som anknyter till kärnområdet i privatlivet, får åtgärden inte vidtas. Kärnområdet i privatlivet utgörs av en persons intima privatliv. Exempelvis en persons familjeliv hör däremot inte i sig till kärnområdet i hans eller hennes privatliv.

Tysklands underrättelsetjänst för utlandet BND får öppna postförsändelser och utföra teleavlyssning, förutom för att upptäcka vissa brott och planer på brott mot den nationella säkerheten, även om det är nödvändigt för att underrättelsetjänsten ska kunna sköta vissa uppgifter som den åläggs i BND-lagen eller för att skaffa information om hot mot liv eller hälsa i fråga om en person som befinner sig utomlands.

G10-lagens 5 § gäller s.k. strategisk begränsning av kommunikationshemligheten (strategische Beschränkungen) dvs. underrättelseinhämtning som avser datatrafik. Enligt bestämmelsen får Tysklands underrättelsetjänst för utlandet BND med tillstånd av det parlamentariska kontrollrådet som verkar i anslutning till förbundskanslersämbetet och förbundsdagen utföra underrättelseinhämtning som avser datatrafik, om det är nödvändigt för att upptäcka vissa hot och för att förhindra dem i god tid innan de sätts i verket. Hot som berättigar till användning av underrättelseinhämtning som avser datatrafik är bl.a. väpnade angrepp mot Tyskland, internationell terrorism, internationell spridning av militära vapen och massförstörelsevapen, yrkesmässig införsel av narkotika, förfalskning av pengar utomlands som hotar euroområdets stabilitet, omfattande organiserad människosmuggling och hot mot liv eller hälsa för en person som befinner sig utomlands. Underrättelseinhämtning som avser datatrafik baserar sig på automatiska sökbegrepp som kan gälla antingen kommunikationens innehåll eller dess identifieringsuppgifter. Screening baserad på sökbegrepp får vid varje enskilt tillfälle riktas mot högst 20 % av Tysklands internationella datatrafik. Sökbegreppen ska definieras såväl i BND:s skriftliga tillståndsansökan som i det skriftliga tillstånd som beviljas av förbundskanslersämbetet och kontrollrådet och vars maximala giltighetstid är tre månader. Sökbegreppen får inte specificera någon enskild teleanslutning och de får inte gälla kärnområdet i privatlivet. Uppgifter som gäller kärnområdet i privatlivet och som eventuellt ändå avslöjas i samband med underrättelseinhämtning som avser datatrafik ska utplånas. Frågan om hur nödvändiga de uppgifter är som inhämtats genom underrättelseinhämtning som avser datatrafik ska bedömas med sex månaders intervall. Om uppgifterna inte är nödvändiga för insamlingssyftet och det inte finns någon grund för att de lämnas ut till en annan myndighet, ska de utplånas. Uppgifter får lämnas ut till

nationella säkerhetstjänster om det finns konkret fog att anta att de är nödvändiga för skötseln av deras fastslagna uppgifter. Dessutom får uppgifter under vissa förutsättningar lämnas ut till myndigheten för exportkontroll. Utlämnande av uppgifter till polis- och åklagarmyndigheter samt utländska myndigheter behandlas under separata rubriker nedan.

Den som är föremål för teleavlyssning och underrättelseverksamhet som avser datatrafik ska underrättas efter det att användningen av informationsinhämtningsmetoden har avslutats. Säkerhets- och underrättelsetjänsterna kan dock skjuta upp underrättelsen, om den skulle kunna äventyra syftet med informationsinhämtningen eller om underrättelsen kan bedömas skada förbundsstatens eller delstaternas allmänna intressen. Om en underrättelse inte har gjorts inom 12 månader efter det att användningen av informationsinhämtningsmetoden har avslutats, ska förutsättningarna för underrättelsen bedömas av myndigheten för laglighetskontroll (G10-kommissionen). Efter det här beslutar kommissionen om längden på uppskovet. Om underrättelsen inte har gjorts inom fem år efter det att användningen av en informationsinhämtningsmetoden avslutades och grunderna för att låta bli att göra en underrättelse fortfarande föreligger och med stor sannolikhet kommer att föreligga även i framtiden, kan G 10-kommissionen enhälligt besluta om att permanent låta bli att göra underrättelsen.

*Rapportering*

Varje säkerhets- eller underrättelsetjänst rapporterar till det ministerium som styr dess verksamhet. Närmare reglering angående uppfyllandet av rapporteringsskyldigheterna ingår i sekretessbelagda reglementen för säkerhets- och underrättelsetjänsterna. I fråga om rapporteringen är det dock även skäl att notera att såväl de styrande ministerierna som det parlamentariska kontrollorganet och organet för laglighetskontroll deltar i beslutsfattandet angående användning av hemliga metoder för underrättelseinhämtning. På så vis får de även via den här kanalen redan på förhand information om vissa enskilda operationer inom säkerhets- och underrättelsetjänsterna.

*Samarbete med brottsbekämpningsmyndigheterna*

I vissa lagar angående underrättelse- och säkerhetstjänsternas verksamhet konstateras uttryckligen att tjänsterna inte har några polisbefogenheter och att de inte har rätt att be polisen att utföra sådana åtgärder för deras räkning som de inte själva har rätt att utföra. Däremot finns det detaljerade bestämmelser om informationsgången mellan säkerhets- och underrättelsetjänsterna samt brottsbekämpningsmyndigheterna.

Säkerhets- och underrättelsetjänsternas skyldighet att rapportera brott till åklagarmyndigheterna och polismyndigheterna fastställs enligt 20 § i BfV-lagen. Lagarna om den militära säkerhetstjänsten MAD och underrättelsetjänsten för utlandet BND hänvisar direkt till den här bestämmelsen. Enligt bestämmelsen har säkerhets- och underrättelsetjänsterna en skyldighet att på eget initiativ till åklagare och polismyndigheter lämna ut alla sådana uppgifter som med fog kan antas behövas för att förhindra och utreda brott samt väcka åtal när det gäller brott som riktar sig mot staten. Brott som riktar sig mot staten är utöver sådana brott som särskilt nämns i vissa lagar även alla sådana straffbara handlingar som kan antas rikta sig mot den grundlagsenliga samhällsordningen i förbundsstaten eller delstaterna, deras existens eller säkerhet eller Tysklands externa säkerhet. Rapporteringsskyldigheten gäller således sådana brott som i stor utsträckning kan anses hänföra sig till säkerhets- och underrättelsetjänsternas egna lagstadgade verksamhetsområden. Polismyndigheterna har däremot rätt att av säkerhets- och underrättelsetjänsterna begära och få information som behövs för förhindrande av sådana brott. De behöver dock inte på eget initiativ och inte heller på begäran lämna ut information som behövs för att

förhindra eller utreda brott eller väcka åtal, om det är motiverat exempelvis med hänsyn till väsentliga säkerhetsintressen att man låter bli att lämna ut informationen.

Skyldigheten att lämna ut information är inte ensidig. Åklagar-, polis- och tullmyndigheterna liksom även förbundsstatens myndigheter har allmänt en skyldighet att på eget initiativ informera säkerhets- och underrättelsetjänsterna om hot som anknyter till deras verksamhetsområde. Säkerhets- och underrättelsetjänsterna har däremot rätt att begära och få information om hot från brottsbekämpningsmyndigheterna och förbundsstatens myndigheter.

Utöver ett ömsesidigt utlämnande av information kan säkerhetsmyndigheterna och brottsbekämpningsmyndigheterna inrätta gemensamma projektvisa personregister då den information som ska föras in i dem anknyter till båda parters uppgifter. Projektvisa personregister kan endast inrättas för en viss tid.

G10-lagen innehåller särskilda bestämmelser om utlämnande av sådana uppgifter till brottsbekämpningsmyndigheterna som erhållits med hjälp av metoder för underrättelseinhämtning som riktas mot innehållet i ett förtroligt meddelande. Uppgifter som erhålls med hjälp av teleavlyssning eller underrättelseinhämtning som avser datatrafik får lämnas ut till åklagar- eller polismyndigheterna endast för förhindrande eller utredning av eller åtal för sådana brott som nämns i en uttömmande förteckning i lagen. De förteckningar som ingår i G10-lagen över brott som utgör grund för ett utlämnande av uppgifter är i sig mycket omfattande. Den förteckning över brottsrubriceringar som finns i anslutning till bestämmelsen om underrättelseinhämtning som avser datatrafik är något knapphändigare än den förteckning som finns i anslutning till bestämmelsen om teleavlyssning. Brotten i båda förteckningarna kan anses rikta sig mot den nationella säkerheten.

*Internationellt samarbete*

De lagar som gäller säkerhets- och underrättelsetjänsternas verksamhet innehåller ingen allmän reglering om internationellt samarbete. Däremot innehåller de bestämmelser om förutsättningar på vilka tjänsterna kan lämna ut information till utländska samarbetsmyndigheter.

Enligt 19 § i BfV-lagen och de relevanta bestämmelser i lagarna angående MAD och BND som hänvisar till paragrafen får säkerhets- och underrättelsetjänsterna lämna ut personuppgifter till utländska myndigheter eller internationella organisationer, om utlämnandet är nödvändigt för att utlämnaren ska kunna fullgöra sina lagstadgade uppgifter eller för att skydda mottagarens viktiga säkerhetsintressen. Uppgifter får däremot inte lämnas ut om det står i strid med Tysklands utrikespolitiska intressen eller med betydande intressen för den person som är föremål för utlämnandet av uppgifter. Händelsen då uppgifterna lämnas ut ska dokumenteras och mottagaren ska informeras om att uppgifterna endast får användas i enlighet med syftet med utlämnandet.

*Ny lagstiftning angående signalspaning som avser utländska förhållanden*

BND:s befogenheter för signalspaning som avser utländska förhållanden kodifierades första gången i en lag (Gesetz zur Ausland-Ausland-Fernmedeaufklärung des Bundesnachrichtendienstes), som trädde i kraft vid ingången av 2017.

En förutsättning för att signalspaning ska kunna genomföras utomlands är enligt den nya lagen att detta är nödvändigt för att upptäcka hot mot förbundsrepublikens interna eller externa säkerhet i ett tidigt skede, för att säkerställa förbundsrepublikens funktionsförmåga eller för att

skaffa uppgifter som vederbörande ministerier har klassificerat som utrikes- och säkerhetspolitiskt viktiga. Signalspaning utomlands ska basera sig på användning av sökbegrepp. Sökbegreppen kan beskriva såväl personer och organisationer som ärenden. På vissa särskilda villkor tillåter lagen underrättelseinhämtning som riktas mot Europeiska unionens institutioner och unionens medlemsstater. Underrättelseinhämtningen får inte kränka kärnområdet i privatlivet. Med kärnområdet i privatlivet avses inte en persons familjeliv eller sociala relationer utan frågor som gäller intimitetens kärna, exempelvis sexualliv. Lagen innehåller ett uttryckligt förbud mot ekonomisk underrättelseinhämtning för att främja tyska intressen i anknytning till näringslivet (Wirtschaftsspionage), men tillåter däremot inhämtning av information av finanspolitisk betydelse.

Beslut om användning av signalspaning utomlands fattas med avvikelse från tidigare inte av underrättelsetjänsten själv utan av förbundskanslersämbetet. Dessutom ska beslut om användning av signalspaning utomlands godkännas på förhand genom försorg av ett oberoende kontrollorgan (Unabhängiges Kontrollgremium) som inrättades genom lagen. Det oberoende kontrollorganet består av en ordförande och två medlemmar. Ordförande och en av medlemmarna ska vara domare vid högsta domstolen (Bundesgerichthof) i förbundsrepubliken Tyskland och en av medlemmarna åklagare vid högsta domstolen. Utöver att organet godkänner beslut som gäller signalspaning övervakar det verksamheten i efterhand bl.a. i form av laglighetskontroller. Organet undersöker även klagomål gällande signalspaning utomlands. Det oberoende kontrollorganet informerar förbundsdagens kontrollråd med minst sex månaders intervall.

Lagen innehåller bestämmelser om internationellt samarbete inom ramen för signalspaning som avser utländska förhållanden. BND får samarbeta med utländska underrättelsemyndigheter under förutsättning att det är nödvändigt för att syftet med signalspaning som avser utländska förhållanden ska nås och att information inte kan inhämtas på annat sätt. Detaljerna för samarbetet ska antecknas i ett samförståndsavtal mellan parterna. Samförståndsavtalet kan endast gälla informationsinhämtning i fråga om internationell terrorism, spridning av massförstörelsevapen eller krigsvapen, utvecklingen i fråga om kriser utomlands, sådana utländska politiska, ekonomiska eller militära utvecklingsförlopp som kan ha betydelse för Tysklands utrikes- och säkerhetspolitik eller andra teman som kan jämställas med ovan nämnda frågor. Dessutom kan samförståndsavtalet gälla nödvändig signalspaning för att stödja tyska försvarsmakten eller dess allierade eller för att bedöma säkerhetssituationen för tyska medborgare eller allierade länders medborgare som befinner sig utomlands.

2.3.2.5 Nederländerna

I Nederländerna ansvarar en allmän underrättelse- och säkerhetstjänst (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) och en militär underrättelse- och säkerhetstjänst (Militaire Inlichtingen- en Veiligheidsdienst, MIVD) för underrättelseverksamheten. Deras verksamhet regleras i en lag om underrättelse- och säkerhetstjänster från 2002 (Wet op de inlichtingen- en veiligheidsdiensten, 2002, nedan WIV-lagen).

*Styrning*

Tjänsterna är underställda ministerierna. Den allmänna underrättelsetjänsten lyder under inrikesministeriet och den militära underrättelsetjänsten under försvarsministeriet. Ministern har självständiga befogenheter i anslutning till verksamheten inom sin egen tjänst (exempelvis beslutsfattande i anslutning till tillståndsansökningar). Ministrarna har befogenheter att utfärda detaljerade regler för organisationen, arbetsmetoder och förvaltningen.

I lag finns bindande bestämmelser om det inbördes samarbetet mellan den civila och militära underrättelsetjänsten. Dessutom förhandlar inrikes- och försvarsministrarna sinsemellan om samordningen av verksamheten. Tjänsterna har en gemensam koordinator, vars uppgift är att bereda förhandlingar mellan ministrarna och koordinera genomförandet av uppgifterna. Koordinatorn är ansvarig för sin verksamhet direkt inför Nederländernas premiärminister.

*Underrättelsetjänsternas uppgifter*

En allmän uppgift för tjänsterna är att de ska främja den nationella säkerheten. I praktiken koncentrerar sig den allmänna underrättelsetjänsten på icke-militära hot och situationsbedömningar såsom extrema rörelser och terrorism då den militära underrättelseinhämtningen koncentrerar sig på militära hot och situationsbedömningar. Tjänsterna har befogenheter för att bedriva underrättelseinhämtning och kontraspionage. Båda tjänsterna kan i sig vara verksamma i hemlandet och utomlands, men den militära underrättelseinhämtningen får använda hemliga informationsinhämtningsmetoder utanför försvarsministeriets utrymmen endast med inrikesministerns tillstånd. Regeringen utfärdar anvisningar om uppgiftsfördelningen och befogenhetsområden i främmande stater.

Den allmänna underrättelsetjänstens uppgift är att undersöka organisationer eller personer som kan misstänkas förorsaka fara för den demokratiska rättsordningen eller statens säkerhet, utföra säkerhetsutredningar, agera för att trygga sådana statliga intressen som är av grundläggande betydelse (exempelvis skydda sekretessbelagda uppgifter), utföra undersökningar som gäller andra länder på uppdrag av regeringen och sammanställa hot- och riskbedömningar.

Den militära underrättelseinhämtningens uppgift är att skaffa information i syfte att bedöma den operativa prestationsförmågan hos andra staters väpnade styrkor, undersöka omständigheter som inverkar eller som kan inverka på upprätthållandet eller främjandet av den internationella rättsordningen, utföra säkerhetsutredningar, utföra undersökningar för att förbättra försvarsmaktens operativa prestationsförmåga (exempelvis för att förhindra verksamhet som skadar, för att främja mobilisering), skydda sekretessbelagda uppgifter, utföra undersökningar på uppdrag av regeringen när det gäller militärt viktiga teman och sammanställa hot- och riskbedömningar.

*Metoder för informationsinhämtning*

Det finns detaljerade bestämmelser om tjänsternas särskilda befogenheter, dvs. hemliga metoder för informationsinhämtning. I lag förtecknas de hemliga metoder för informationsinhämtning som står till tjänsternas förfogande. Sådana är observation, teknisk observation, teleövervakning, täckoperationer, hemliga genomsökningar, hemligt öppnande av postförsändelser, intrång i datatekniska miljöer och underrättelseinhämtning som riktas mot datatrafik. I fråga om underrättelseinhämtning som riktas mot datatrafik är det värt att beakta att lagen gör skillnad mellan datatrafik i tråd och utanför tråd.

De krav som ställs på hanteringen av uppgifter är avgörande för användningen av särskilda befogenheter och samarbetet med brottsbekämpningsmyndigheter eller främmande staters underrättelsemyndigheter. Kraven gäller ändamålsbundenhet, nödvändighet, omsorgsfullhet, tillbörlighet samt tillförlitlighet i fråga om uppgiftshanteringen. Hantering av personuppgifter får endast anknyta till en misstanke om äventyrande av den demokratiska rättsordningen eller statens säkerhet, ett tillstånd som en person har gett, en nödvändig orsak som anknyter till en undersökning, erhållande av uppgifter från en främmande stats underrättelse- eller säkerhetstjänst eller en klanderfri skötsel av uppgifter.

Användingen av särskilda befogenheter begränsas i artikel 6.2 i lagen enligt vilket den allmänna underrättelsetjänsten får använda särskilda befogenheter som definieras i lag endast för undersökningar som anknyter till äventyrande av den demokratiska rättsordningen, statens säkerhet eller främmande stater. På motsvarande sätt är befogenheterna för den militära underrättelseinhämtningen bundna till informationsinhämtning om främmande staters prestationsförmåga, förbättrandet av prestationsförmågan och skydd av sekretessbelagda uppgifter i enlighet med artikel 7.2 i lagen.

Användningen av särskilda befogenheter är bunden till de principer som avses i artikel 31. Enligt artikeln ska i främsta hand användas uppgifter som finns i offentliga källor eller i något annat ämbetsverk (subsidiaritetsprincipen), ska tjänsterna använda den informationsinhämtningsmetod som förorsakar minsta olägenhet (principen om minsta olägenhet), får särskilda befogenheter inte användas så att de förorsakar oskälig olägenhet (skälighetsprincipen) och ska användningen stå i rätt proportion till det mål som eftersträvas (proportionalitetsprincipen). Artikel 32 förutsätter att användningen av befogenheten ska avslutas omedelbart då målet för användningen har uppnåtts eller om målet kan uppnås med en metod som förorsakar mindre olägenhet.

Artikel 13.1 i lagen om telekommunikation (Telecommunicatiewet) förpliktar teleoperatörerna att sköta det tekniska genomförandet som anknyter till kommunikationen så att det är möjligt att utföra teleövervakning. Teleoperatörerna är också skyldiga att hjälpa till med det tekniska genomförandet av teleövervakning.

Enligt artikel 13.6 i lagen om telekommunikation ansvarar teleoperatörerna på egen bekostnad för genomförandet av de tekniska åtgärderna, verksamheten och underhållet utan särskild ersättning. Däremot kan teleoperatörerna ansöka om ersättning för sådana person- och förvaltningskostnader som föranleds av genomförandet av teleövervakning eller av att de svarar på begäran om information. Artiklarna 28 och 29 i lagen om underrättelsetjänster ger underrättelsetjänsterna möjligheter att få uppgifter om användarna och användarnas teletrafik av teleoperatörerna. Uppgifterna kan innehålla information om användarens grundläggande uppgifter, kontakter, datakommunikation med kontakter och användarens avtal om datatrafik samt betalningstrafik.

I WIV-lagen ingår ingen allmän tidsfrist för bevarandet av insamlade uppgifter. Utplånandet styrs generellt enligt artikel 43 enligt vilken uppgifter som saknar betydelse för utredningen ska utplånas. Uppgifter som har lagrats under icke inriktad övervakning av datatrafik som avses i artikel 27 kan bevaras under ett års tid för sortering. Personer som blivit föremål för öppnande av postförändelser, övervakning av datatrafik och intrång i utrymmen ska underrättas inom fem år efter det att användningen av dessa befogenheter har avslutats. Anmälningsskyldigheten förfaller om det inte går att utreda vilken person som blivit föremål för åtgärderna eller om underrättandet kan äventyra intressen som anknyter till underrättelsetjänstens metoder, källor eller internationella relationer.

*Rapportering*

De ministrar som ansvarar för underrättelseverksamheten avger årligen en berättelse till båda kamrarna i parlamentet (Staten-Generaal) om underrättelsetjänsternas verksamhet. I berättelsen ska nämnas insatsområdena åtminstone för det föregående och det kommande året. Det är inte nödvändigt att redogöra för tekniska uppgifter eller den faktiska nivån för uppgifterna.

Dessutom har ministrarna ålagts att på eget initiativ rapportera till parlamentet. Åtminstone sådan sortering som baserar sig på sökord ska anmälas konfidentiellt till båda kamrarna i parlamentet samt till granskningskommittén.

Underrättelseverksamheten övervakas av en extern granskningskommitté (CTIVD), som övervakar lagenligheten i verksamheten, utför kontroller och rapporterar samt behandlar klagomål i en rådgivande roll. Parlamentarisk övervakning utförs av ett utskott för säkerhets- och underrättelsefrågor i parlamentets underhus, och till den del det är möjligt när det gäller offentliga handlingar, av representanthusets utskott för inrikesärenden.

*Samarbete med brottsbekämpningsmyndigheterna*

Underrättelsetjänsterna har inga befogenheter att utreda brott utan deras verksamhet koncentreras till insamling av information och analyser av hot. Tjänsterna samarbetar med andra organisationer.

Samarbetet med brottsbekämpningsmyndigheterna är ömsesidigt och baserar sig på utbyte av uppgifter och tekniskt stöd. Tjänsterna kan till åklagarmyndigheterna lämna ut sådana uppgifter som kan ha betydelse för utredning av brott eller väckande av åtal. Beslut om utlämnande av uppgifter fattas av ministern eller den chef för tjänsten som handlar i ministerns namn. Utlämnande av uppgifter ska vara nödvändigt för att åklagarmyndighetens lagstadgade uppgift ska kunna fullgöras. Enligt förarbetena ska tjänsterna överväga intresset att reda ut ett brott mot intressen som gäller den nationella säkerheten. Tjänsterna behöver inte lämna ut uppgifter, om utlämningen allvarligt skadar deras intressen. Brottsbekämpningsmyndigheterna kan begära tekniskt stöd av tjänsterna.

*Internationellt samarbete*

Tjänsterna bedriver aktivt internationellt samarbete antingen för att upprätthålla samarbetsförbindelser eller för att utföra tjänstens egna lagstadgade uppgifter. Tjänsterna får lämna ut och ta emot uppgifter (inkl. personuppgifter) samt tekniskt stöd. Enligt lagens förarbeten ska tjänsterna bedöma samarbetet utifrån Nederländernas utrikespolitik och situationen angående de mänskliga rättigheterna i en främmande stat. Samarbetet får inte stå i strid med sådana intressen som tjänsterna tryggar och samarbetet får inte heller förhindra en klanderfri skötsel av tjänsternas lagstadgade uppgifter. Cheferna för tjänsterna upprätthåller gemensamt relationer till underrättelse- och säkerhetsmyndigheter i andra stater.

Tjänsterna ska följa samma regler då de ger tekniskt stöd som även i övrigt, vilket även gäller användningen av särskilda befogenheter. Ministern fattar beslut om givandet av stöd. Lagen innehåller inga uttryckliga bestämmelser om hur hjälp begärs av andra underrättelsetjänster, men tjänsterna kan exempelvis begära att en främmande stats underrättelsetjänst följer ett specifikt objekt i den främmande staten.

Underrättelsetjänsterna i Nederländerna får lämna ut uppgifter till en underrättelsetjänst i utlandet på det villkor att den mottagande tjänsten inte lämnar ut uppgifterna till en tredje part. Det här gäller även då tjänsterna tar emot uppgifter från en främmande stat. Avvikelse från detta kan göras med tillstånd av ministern.

*Anhängiga lagstiftningsprojekt i Nederländerna*

Beredningen av en lag som ska ersätta 2002 års lag har pågått sedan 2013, då Dessens kommission som tillsattes för att bedöma lagstiftningen avgav sin rapport. Syftet med det anhängiga lagförslaget är att ge underrättelsetjänsterna nya befogenheter, förlänga den tid de insamlade uppgifterna ska bevaras, förbättra den rättsliga övervakningen samt mer allmänt att uppdatera lagstiftningen för att den ska motsvara den teknologiska utvecklingen. Lagförslaget innehåller förslag till utveckling av underrättelseinhämtningen som avser datatrafik, exempelvis att särskiljandet mellan datatrafik i tråd och utanför tråd ska slopas. I lagförslaget föreslås även en samarbetsförpliktelse för teleoperatörerna. Enligt lagförslaget är användningen av särskilda befogenheter bunden till att tillstånd erhålls från ett nytt rättsligt organ.

Det nederländska parlamentets underhus röstade om lagsförslaget den 9 februari 2017 och parlamentets överhus antog lagen den 12 juli 2017. Lagen föreslogs träda i kraft den 1 januari 2018. Efter att parlamentets överhus hade antagit lagen ordnades det emellertid en folkomröstning om lagen och det är således ännu öppet vid vilken tidpunkt lagen träder i kraft.

2.3.2.6 Schweiz

Det schweiziska parlamentet godkände i september 2015 ett förslag till ny lag om underrättelseinhämtning, som fastställer uppgiftsbeskrivningen för den nationella underrättelsetjänsten (Nachrichtendienst des Bundes; NDB) och ändrar befogenheterna för tjänsten. De mest omfattande ändringarna gäller att övervakning av privata utrymmen blir tillåten samt övervakning av gränsöverskridande datatrafik. Ändringarna kommer att utvidga befogenheterna för militär underrättelseinhämtning genom vissa hänvisningsbestämmelser. Det ordnades en folkomröstning om lagen den 26 september 2016 då lagen godkändes. Den nya lagen om underrättelseinhämtning trädde i kraft den 1 september 2017.

Den nya lagen om underrättelseinhämtning ersätter som allmän lag gällande lag om metoder för säkerställande av den inre säkerheten (loi fédérale instituant des mesures visant au maintien de la sûreté intérieure; LIMS) och gällande lag om civil underrättelseinhämtning (loi fédérale sur le renseignement civil; LFRC).

*Styrning*

Enligt den nya lagen styrs underrättelsetjänsten politiskt av Schweiz förbundsförsamling. Till förbundsförsamlingens uppgifter hör bl.a. att ge underrättelsetjänsten en sekretessbelagd primär uppgift, som förnyas med minst fyra års intervall, samt att årligen godkänna en lista över organisationer och sammanslutningar som ska observeras. Dessutom beslutar förbundsförsamlingen om nödvändiga åtgärder i särskilda hotsituationer.

*Underrättelsetjänstens uppgift*

Enligt den nya lagen är det underrättelsetjänstens uppgift att identifiera och i tid förhindra hot som riktas mot den interna och externa säkerheten med anknytning till terrorism, våldsbejakande extremiströrelser, spionage, olaga handel med krigsmateriel och vapen samt skydd av kritisk infrastruktur. Underrättelsetjänsten ska garantera landets intressen och verksamhetsförmåga. Uppgifterna omfattar befogenheter med avseende på utlandet och underrättelsetjänsten ska bedöma händelser utomlands som är av säkerhetspolitisk betydelse. Lagen innehåller en undantagsparagraf, som då allvarligt och direkt hot föreligger, gör det möjligt att genom beslut av regeringen tillämpa lagen även för att stödja den schweiziska utrikespolitiken och skydda den konstitutionella ordningen, industrin, ekonomin och finanssektorn.

Den huvudsakliga uppgiften för underrättelsetjänsten är att för det politiska beslutsfattandet ge ut förberedande varningar för faktorer som hotar den nationella säkerheten. I egenskap av ett säkerhetspolitiskt instrument stöder NDB dessutom främst regeringen, ministerierna samt försvarsministeriets ledning. Dessutom stöder NDB kantonerna när det gäller att bevara den interna säkerheten samt åklagarmyndigheterna. Utöver den statliga underrättelsetjänsten NDB har även den schweiziska försvarsmakten en egen underrättelsetjänst (Militärischer Nachrichtendienst; MND), som NDB samarbetar med.

*Informationsinhämtningsmetoder och hur beslut fattas om dem*

Lagen om försvarsmakten (Loi Fédérale sur l'armée et administration militaire) innehåller bestämmelser om underrättelseuppdraget för försvarsmaktens underrättelsetjänst och det preciseras i en förordning om elektronisk krigföring och radiosignalspaning (Ordonnance sur la guerre électronique et l'exploration radio). En militärunderrättelsemyndighet kan utföra signalspaning med stöd av ovan nämnda bestämmelser och med stöd av civila underrättelsemyndigheters befogenheter för radiospaning. Försvarsmakten har ett centrum för elektroniska operationer (COE) som utför signalspaning i Schweiz.

Enligt den nya lagen är det tillåtet att utföra underrättelseinhämtning som avser datatrafik endast om antingen mottagaren eller avsändaren befinner sig utomlands. Underrättelsetjänsten ska få tillgång till uppgifter från signaler endast om uppgifterna motsvarar givna sökord. Sökorden ska enligt lagen avgränsas så att de kränker integritetsskyddet i så liten omfattning som möjligt och de får inte heller innehålla namn på schweiziska fysiska eller juridiska personer. Om det finns ett tillstånd för underrättelseinhämtning som avser datatrafik, är kabel- och nätverksoperatörer enligt den nya lagen skyldiga att lämna ut signalerna till COE som är underställt försvarsmakten. Dessutom skaffar COE alla nödvändiga tekniska installationer för att dess uppgifter ska kunna utföras samt genomför nödvändiga skeden och tester. COE kan också inom ramen för sitt uppdrag föreslå att underrättelseinhämtningen inriktas på nytt. COE kan utföra underrättelseinhämtning på elektronisk strålning som kommer från datasystem i utlandet.

Enligt den nya lagen kan underrättelsetjänsten ansöka om tillstånd för vissa åtgärder, om det finns ett konkret internt eller externt hot som exempelvis beror på terrorism. Tillstånd krävs för övervakning av post- och teletrafik, applicering av positionsbestämningsutrustning på personer och föremål, positionsbestämning av föremål, husrannsakan av bilar och utrymmen, montering av övervakningsanordningar i privata utrymmen samt intrång i datasystem och datanät för att få information eller för att förhindra tillgång till information. Datorer eller datanät som finns utomlands skulle man kunna påverka om de används för angrepp mot den kritiska infrastrukturen i Schweiz. Det ska vara möjligt att övervaka datatrafik som överskrider Schweiz geografiska gränser utifrån noggrant definierade sökord. En förutsättning för beviljande av tillstånd att använda sådana metoder är bl.a. att andra underrättelseinhämtningsåtgärder har varit resultatlösa. Kabel- och nätverksoperatörer har rätt till en monetär ersättning som beviljas av staten. Regeringen fastställer ersättningen enligt storleken på de kostnader utlämnandet av uppgifter till centret för elektroniska operationer har förorsakat.

Enligt den nya lagen ska tillstånd för åtgärderna sökas hos förvaltningsdomstolen och därefter beviljar försvarsministern tillstånd att inleda verksamheten efter att först skriftligen ha konsulterat såväl utrikes- som justitieministern. Särskilt betydande fall kan föras till förbundsförsamlingen för behandling. Lagen medger även att chefen för underrättelsetjänsten i en nödsituation brådskande får godkänna tillståndspliktig övervakning. Tillståndet ska dock utan dröjsmål även ansökas enligt normalt förfarande och åtgärderna kan vid behov även avbrytas. Tillstånd

för användning av befogenheter utomlands beviljas alltid av förbundsförsamlingen. I alla beslut som förbundsstatens myndigheter har fattat med stöd av lagen om underrättelseinhämtning kan ändring sökas hos förbundsstatens förvaltningsdomstol.

NBD kan genom skriftliga eller muntliga förfrågningar selektivt skaffa information som den behöver för att sköta sina uppgifter. NBD kan sända personer en skriftlig förhörskallelse, men den person som uppgifterna begärs av ska informeras om att uppgiftslämnandet är frivilligt. Ett undantag från detta är informationsinhämtning genom täckoperationer. Om det är nödvändigt för att upptäcka, förhindra eller avvärja ett konkret hot, kan NBD även kräva uppgifter och upptagningar a) av sådana fysiska eller juridiska personer som yrkesmässigt sköter transporter eller förmedlar eller ställer transportmedel till förfogande och b) av privata leverantörer av säkerhetsinfrastruktur, såsom utrustning för bildöverföring och -lagring.

Enligt lagen är det tillåtet att använda drönare och satelliter. Utan särskilt tillstånd kan underrättelsetjänsten dessutom använda offentliga informationskällor (medier, uppgifter som privata har lagt fram offentligt, statliga myndigheters och kantonernas myndigheters offentliga register samt i offentligheten framförda uttalanden), använda personer som informationskällor, anmäla personer och fordon i polisens efterlysningssystem, övervaka och inspela bild och ljud i offentliga utrymmen.

Den nya lagen medger även att man vid behov med tillstånd av chefen för underrättelsetjänsten skapar en täckidentitet för att skydda en arbetstagare vid underrättelsetjänsten. Med försvarsministerns tillstånd kan man skapa en täckidentitet för en arbetstagare.

Terroristorganisationer och organisationer med våldsframtoning kan förbjudas bedriva verksamhet i Schweiz. Den nya lagen om underrättelseinhämtning kommer att innehålla en paragraf med stöd av vilken organisationer kan förbjudas helt och hållet för fem år åt gången. Enligt lagen har underrättelsetjänsten inte rätt att ingripa exempelvis i politisk aktivitet eller utövandet av yttrandefrihet. Ett undantag från detta är konkret misstanke om terrorism eller radikalisering.

Lagen innehåller även bestämmelser om en skyldighet att utplåna personuppgifter senast i det skede då de misstankar som utgjort grund för åtgärden har kunnat uteslutas. Om det inte går att bevisa terrorism eller radikalism, ska personuppgifterna utplånas senast ett år efter att utredningen påbörjades. I fråga om försvarsmaktens signalspaning finns det en avvikande bestämmelse angående utplåning av uppgifter. Meddelandena ska utplånas inom 18 månader och förmedlingsuppgifterna för meddelandena inom fem år efter att man fått dem i sin besittning.

Underrättelsetjänsten är skyldig att informera en person som har blivit föremål för en underrättelseinhämtningsåtgärd om övervakningen senast inom en månad efter att övervakningen avslutats. Av vägande skäl kan man dock med tillstånd skjuta upp delgivningen eller avstå från den helt och hållet.

*Rapportering*

Det ministerium som har hand om frågor som gäller försvar, befolkningsskydd och idrott sammanställer årligen en plan angående lagligheten, ändamålsenligheten och effektiviteten i underrättelsemyndighetens verksamhet och tillsätter ett internt kontrollorgan för allmän övervakning. Detta organ informerar fortgående chefen för ministeriet om övervakningsverksamhetens resultat. Dess rapporter är inte offentliga. Det förutsätts enligt lag att ministeriet regelbundet rapporterar till förbundsförsamlingen om sin underrättelseverksamhet.

Enligt lag ska chefen för underrättelsetjänsten årligen särskilt rapportera om användningen av täckidentiteter till försvarsministeriet.

*Samarbete med brottsbekämpningsmyndigheterna*

Enligt lag ska underrättelsetjänsten sända personuppgifter till de schweiziska myndigheterna då upprätthållandet av den interna eller externa säkerheten kräver det. Då NBD har uppgifter som är till nytta för andra myndigheter i straffrättsliga förfaranden, för att förhindra brott eller upprätthålla allmän ordning, ska NBD lämna ut dessa uppgifter för ifrågavarande myndigheters bruk med iakttagande av källskyddet. NBD tillställer brottsbekämpningsmyndigheterna sådana uppgifter som inhämtats med tillståndspliktiga metoder endast om de innehåller någonting konkret som tyder på ett brott där lagföringen kan ge anledning till straffrättsliga åtgärder. Det fortsatta förfarandet sker i enlighet med straffprocesslagen eller lagen angående krigsbrottsprocesser.

*Internationellt samarbete*

Den nya lagen om underrättelseinhämtning gör det även möjligt att bedriva samarbete med utländska underrättelsetjänster och säkerhetsmyndigheter bl.a. när det gäller att skaffa information samt för att kunna skapa en hotbild. Samarbete utförs inom gränserna för den politiska styrningen. Förbundsstatens övriga myndigheter samt kantonernas myndigheter får upprätthålla förbindelser med utländska underrättelsetjänster eller andra utländska myndigheter för att fullgöra de underrättelseuppdrag som avses i denna lag endast med NBD:s medgivande eller genom NBD. På det militära området kan NBD i internationella sammanhang bedriva samarbete med arméns ansvariga enheter, begära uppgifter av myndigheterna och ge dem uppdrag som anknyter till internationellt samarbete.

Underrättelsetjänsten kan ta emot och förmedla ändamålsenliga uppgifter, arrangera gemensamma överläggningar och sammanträden, genomföra gemensamma insatser för att inhämta och utvärdera information samt för att göra upp hotbedömningar och ta del av internationella automatiserade informationssystem. Vidare kan underrättelsetjänsten skaffa information och förse de stater med information som har lämnat en begäran om det för att man ska kunna bedöma om en enskild person kan delta i säkerhetsklassificerade projekt utomlands som gäller intern eller extern säkerhet eller om en enskild person kan få tillgång till säkerhetsklassificerade uppgifter, material eller utrustning.

Enligt den nya lagen kan NBD i samförstånd med det schweiziska utrikesministeriet sända sina arbetstagare till schweiziska beskickningar utomlands i syfte att förbättra de internationella kontakterna. De som är anställda av NBD arbetar för verkställigheten av lagen direkt med de behöriga myndigheterna i den mottagande staten och i tredjeländer.

## 2.4 Bedömning av nuläget

### 2.4.1 Allmänt

Såsom konstateras i beskrivningen av nuläget har Finlands säkerhetspolitiska miljö förändrats. Detta innebär att det är allt viktigare att den högsta statsledningen har möjlighet att få rättidig, tillförlitlig och oberoende information som stöd för sitt beslutsfattande.

Det finns inga uttryckliga bestämmelser i lag om försvarsmaktens informationsinhämtning för underrättelsesyften, dvs. om militär underrättelseinhämtning. Militär underrättelseinhämtning

har behandlats endast i förarbeten till lag, i regeringens proposition med förslag till lag om försvarsmakten samt vissa lagar som har samband med den (RP 264/2006 rd). I Finland finns inte heller något regelverk om vad man eftersträvar med underrättelseverksamheten eller hurdan underrättelseverksamhet som får bedrivas. Försvarsmaktens – exempelvis Skyddspolisens – befogenheter att inhämta information är otillräckliga med hänsyn till verksamhetens samhälleliga betydelse och i jämförelse med andra länders befogenheter.

I nuläget är befogenheterna begränsade till verksamhet för att förhindra och avslöja brott. Den gällande lagstiftningen möjliggör således inte för säkerhetsmyndigheterna att inhämta information annat än vid misstanke om brott, där föremålet för informationshämtningen alltid är en specificerad person och dennes verksamhet som har samband med brott.

Försvarsmaktens praktiska verksamhet fokuserar på vissa hemliga metoder för att inhämta information i syfte att förhindra och avslöja brott, som regleras i polislagen. Brottsbekämpningsuppdragen gäller endast olovlig underrättelseverksamhet på försvarsområdet och verksamhet som äventyrar det militära försvaret, och för förundersökningen i dessa fall ansvarar inte försvarsmakten utan Skyddspolisen.

Militärt kontraspionage är verksamhet för att skydda landet mot informationsinhämtning som främmande staters underrättelsetjänster, enskilda personer eller organisationer riktar mot försvarsmakten eller mot företag som försvarsmaktens samarbetar med inom projekt och i utvecklings- och forskningsverksamhet. Det militära kontraspionaget är en del av den mer övergripande underrättelseinhämtningen och har i enlighet med sina befogenheter också i uppdrag att inhämta sådan betydelsefull underrättelseinformation som inte syftar till att förhindra eller avslöja brott.

I den föränderliga säkerhetspolitiska miljön kan den militära underrättelseinhämtningen inte i tillräcklig utsträckning stödja den högsta statsledningen i det utrikes-, säkerhets- och försvarspolitiska beslutsfattandet och ha beredskap att avvärja allvarliga säkerhetshot som riktas mot Finland.

Även om de hemliga metoderna för inhämtande av information också kan användas för att förhindra förberedelse till brott och därmed har ett brett användningsområde, är det klart att dessa hemliga metoder för närvarande inte kan användas för att inhämta ren underrättelseinformation om sådan verksamhet som hotar den militära eller nationella säkerheten som inte ännu har utvecklats till förberedelse till brott eller som inte är kriminaliserad verksamhet. Också den militära underrättelseinhämtningens tredje dimension, dvs. informationsinhämtning som sker utanför Finlands gränser och som avser objekt som är betydelsefulla med tanke på Finlands nationella säkerhet, bör beaktas.

Det har blivit allt svårare att avgränsa hot och risker som regionala eller lokala, eftersom ekonomiska, tekniska och sociala system är gränsöverskridande och beroende av varandra. De faktorer som utgör de största hoten mot landets säkerhet anknyter numera ofta till händelser utanför landets gränser. Det blir därmed allt mer sannolikt att följderna av olika hot med utländskt ursprung realiseras i vårt land. Av denna anledning är det svårare än tidigare att föregripa hoten.

De militära hoten har under de senaste åren i stor utsträckning ändrat karaktär. Utöver traditionell militär verksamhet omfattar de moderna militära insatserna olika asymmetriska metoder. I dag kan militära insatser tidsmässigt inledas redan i fredstid med påtryckning och disinformation samt med cyberattacker. På så sätt kan en främmande aktör medvetet försöka på-

verka beslutsfattandet i en annan stat för att nå sådana strategiska mål som staten i fråga inte annars skulle gå med på. De icke-statliga aktörernas påverkningsmöjligheter har ökat också vid militära insatser i och med att tekniken har utvecklats och samhällenas sårbarhet ökat.

På grund av denna förändring i omvärlden har Finlands militära underrättelseinhämtning sämre möjligheter att samla in underrättelseinformation. De nya hottyperna kräver allt snabbbare reaktionsförmåga av statsledningen och försvarsmakten. En adekvat reaktionsförmåga å sin sida kräver tillgång till tillförlitlig information i realtid som stöd för beslutsfattandet. Den militära underrättelseinhämtningen har en central roll vid framtagandet av sådan information.

Att cyberhot och kommunikation som gäller eventuella hot upptäcks och entiteterna bakom hoten identifieras samt att hotets art klarläggs är en förutsättning för att man ska kunna förhindra gärningar som äventyrar den nationella säkerheten eller ha beredskap för sådana gärningar. Den som ansvarar för den förebyggande verksamheten bör i ett så tidigt skede som möjligt få information om hot eller om kommunikation som gäller hot.

Samhället har blivit en miljö där nästan alla traditionella tjänster och aktiviteter styrs av informationsteknik eller helt och hållet sker i informationsnät. Också de militära organisationernas kommunikation sker i och med digitaliseringen i allt större utsträckning i telekommunikationsnät.

För att vara effektiv i en omvärld där informationstekniken tar allt större plats bör dagens underrättelseinhämtning fokusera på digital information. Detta förutsätter att den militära underrättelseinhämtningen ges nya befogenheter på lagnivå.

I november 2013 bekräftade Finlands utrikesministerium uppgifter om att Finlands utrikesförvaltning varit föremål för en allvarlig kränkning av informationssäkerheten. Frågan utreddes i samarbete med Skyddspolisen, som ansvarade för förundersökningen. Enligt Skyddspolisen spionerade två olika stater på utrikesministeriet vid två separata attacker. De finländska myndigheterna fick ursprungligen kännedom om spioneriet vid ingången av 2013 genom en tredje stat. Vid det laget hade det misstänkta spioneriet redan pågått i flera år. I samband med att Skyddspolisen utredde den första incidenten upptäcktes en annan, ännu allvarligare incident. Skyddspolisen utredde det ena dataintrånget som spioneri och det andra som grovt spioneri. Att myndigheterna är tvungna att agera utifrån information från en tredje stat är ohållbart. Om myndigheterna gavs adekvata befogenheter att genomföra underrättelseinhämtning som avser datatrafik, skulle de ha större chanser att upptäcka fall av spioneri och reagera på dem.

### 2.4.2 Föremålen för informationsinhämtning

På grund av den förändrade säkerhetspolitiska miljön är det allt viktigare att Finlands högsta statsledning har möjlighet att få rättidig, tillförlitlig och oberoende information som stöd för sitt beslutsfattande.

I Finland finns inte heller något regelverk om vad man eftersträvar med underrättelseverksamheten eller i vilka situationer underrättelseverksamhet är ändamålsenligt. Försvarsmaktens befogenheter att inhämta information är otillräckliga med hänsyn till verksamhetens samhälleliga betydelse och i jämförelse med andra länders befogenheter.

Finland kan inte anses utgöra ett undantag i det hänseendet att Finland inte skulle vara föremål för främmande staters underrättelseverksamhet eller finskt territorium inte användas för sådan

underrättelseverksamhet, eller att det inte skulle finnas främmande staters underrättelseaktörer på finskt territorium.

I nuläget kan de finländska myndigheterna inte på ett heltäckande sätt hämta in information om verksamhet som främmande staters underrättelseaktörer bedriver på finskt territorium.

Genom informationsinhämtning som sker utifrån misstanke om brott kan man inte inhämta information för sådana behov inom försvarsmakten som avser information om annan verksamhet än verksamhet som kan betraktas som brottslig. Med de befogenheter som grundar sig på misstanke om brott kan försvarsmakten inte inhämta information från utlandet eller inom landet i syfte att sköta sina lagstadgade uppgifter. Information som syftar till att skapa och upprätthålla en militärstrategisk lägesbild av Finlands säkerhetspolitiska miljö och ge förvarning om militära hot under uppsegling kan inte inhämtas i en omfattning som gör det möjligt att i tillräckligt god tid vidta behövliga militära motåtgärder eller motåtgärder som grundar sig på misstanke om brott. Utan misstanke om brott kan man inte inhämta information om t.ex. 1) verksamhet och förberedelse för verksamhet som en främmande stats väpnade styrkor och med dem jämförbara organiserade trupper utför, 2) underrättelseinsatser som riktas mot Finlands försvar, 3) planering, tillverkning, spridning och användning av massförstörelsevapen, 4) utvecklande och spridning av en främmande stats militärmateriel, 5) kriser som hotar internationell fred och säkerhet, 6) verksamhet som hotar säkerheten vid internationella krishanteringsinsatser, 7) hot som riktas mot säkerheten när Finland ger internationellt bistånd och i annan internationell verksamhet som Finland deltar i. Dessutom kan man inte inhämta information om statens verksamhet eller annan sådan verksamhet som kan äventyra det finska försvaret eller samhällets vitala funktioner

I den föränderliga säkerhetspolitiska miljön kan den militära underrättelseinhämtningen inte i tillräcklig utsträckning stödja den högsta statsledningen i det utrikes-, säkerhets- och försvarspolitiska beslutsfattandet eller ha beredskap att avvärja allvarliga säkerhetshot som riktas mot Finland.

Även om de hemliga metoderna för inhämtande av information också kan användas för att förhindra förberedelse till brott och metoderna därmed har ett brett användningsområde, är det klart att dessa hemliga metoder för närvarande inte kan användas för att inhämta ren underrättelseinformation om sådan verksamhet som hotar den militära eller nationella säkerheten som inte ännu har utvecklats till förberedelse till brott eller som inte är kriminaliserad verksamhet.

### 2.4.3 Försvarsmaktens befogenheter att inhämta information

Försvarsmaktens verksamhet för att förhindra och avslöja brott bedrivs i nuläget i synnerhet genom myndighetssamarbete och utredning av händelseförlopp. Verksamheten fokuserar på individer eller händelser som misstänks ha samband med fientliga säkerhets- och underrättelsetjänsters verksamhet. I den förebyggande verksamheten ingriper man i den fientliga verksamheten innan den inleds. I den avslöjande verksamheten samlar man in relevant information om den verksamhet som bedrivits eller om en pågående verksamhet, exempelvis gärningsmannen samt tiden och platsen för gärningen.

För närvarande förfogar inte försvarsmakten över alla de befogenheter som skulle behövas för att inhämta information i syfte att utföra försvarsmaktens lagstadgade uppgifter. Även om försvarsmakten vid behov kan få handräckning av polisen när det gäller att inhämta information utifrån misstanke om brott, kan det inte anses vara ändamålsenligt att försvarsmakten använder en annan myndighets resurser för sin egen verksamhet. Information som hämtas inom ra-

men för militär underrättelseinhämtning kan dessutom behövas för försvarsmaktens beredskap vid krissituationer. I sådana fall kan det inte anses vara lämpligt att polisen anförtros sådana uppdrag. Det som sägs ovan accentueras i synnerhet i situationer där beredskapen kanske behöver höjas och den andra myndighetens resurser eventuellt är bundna till verksamhet som hänför sig till myndighetens egna uppgifter (RP 187/2016, FsUB 1/2017 rd och FsUU 8/2016 rd).

Med hemliga metoder för inhämtande av information kan man inte tillräckligt effektivt och tidigt upptäcka militär verksamhet eller andra föremål för militär underrättelseinhämtning eller vidta åtgärder utifrån den informationen, eftersom användningen av hemliga metoder för inhämtande av information i lagstiftningen är bunden till brott (förhindrande eller avslöjande). Verksamheten fokuserar på individer eller händelser som misstänks ha samband med fientliga säkerhets- och underrättelsetjänsters verksamhet. I den avslöjande verksamheten samlar man in relevant information om den verksamhet som bedrivits eller om den pågående verksamheten, exempelvis information om gärningsmannen samt tiden och platsen för gärningen.

För att försvarsmakten ska kunna identifiera och ha beredskap för eventuella militära och andra yttre hot mot Finland och dess befolkning och kunna avvärja dessa hot, bör försvarsmakten ha möjlighet att utifrån sina egna befogenheter inhämta information om föremålen för den militära underrättelseinhämtningen och skydda Finland samt upprätthålla säkerheten. Den verksamhet som informationsinhämtningen riktar sig mot är i många fall inte kriminaliserad eller också är den inte så långt framskriden att det vore möjligt att rikta en konkret och specifik brottsmisstanke mot verksamheten. Information behövs t.ex. om utvecklingen i den säkerhetspolitiska miljön och om verksamhet som allvarligt hotar staten eller grundläggande samhällsfunktioner, såsom militär verksamhet eller utländska underrättelsetjänsters verksamhet. Lagen om militär disciplin och brottsbekämpning inom försvarsmakten har visat sig vara användbar när det gäller att förhindra och avslöja brott, om än inte till alla delar tillräcklig med tanke på en ändamålsenlig skötsel av uppgifterna.

I militära krishanteringsinsatser som omfattar multinationella insatser kan det inom ramen för insatsens mandat eventuellt också vara möjligt att genomföra personbaserad underrättelseinhämtning. Sådana insatser utgör ett undantag från den informationsinhämtning som grundar sig på misstanke om brott. Utöver detta kan underrättelseverksamhet bedrivas för egenskydd av trupper.

Försvarsmakten förfogar även över metoder för inhämtande av information med vilka man kan inhämta information som betraktas som underrättelseinformation men som inte kräver någon särskild författningsgrund. Sådana metoder är underrättelseinhämtning ur öppna källor samt sådana bildunderrättelser som inte kränker underrättelseobjektens integritetsskydd eller sekretessen beträffande förtroliga meddelanden. Också radiosignalspaning är alltjämt en viktig del av den militära underrättelseinhämtningen. På grund av metoderna och föremålen för radiosignalspaningen har det i fråga om sådan spaning inte krävts några uttryckliga befogenhetsbestämmelser; radiosignalspaning kränker inte sekretessen beträffande förtroliga meddelanden och spaningsobjekten är utländska väpnade styrkor.

Den nationella säkerheten är en av de hänsyn utifrån vilka man enligt artikel 8 i europeiska människorättskonventionen får ingripa i integritetsskyddet. Staterna har rätt omfattande prövningsmarginal i fråga om verksamhet som de anser utgöra ett hot mot den nationella säkerheten. På basis av Europadomstolens avgörandepraxis hör åtminstone det militära försvaret och bekämpningen av olovlig underrättelseverksamhet till den nationella säkerheten. Den nationella säkerheten kan emellertid utsättas för många slags hot som är svåra att förutse eller defi-

niera på förhand. Av detta följer enligt domstolen att begreppet nationell säkerhet i första hand ska preciseras utifrån nationell praxis (Kennedy mot Förenade konungariket, 18.5.2010).

Enligt den arbetsgrupp för informationsinhämtning som dryftat riktlinjerna för underrättelselagstiftningen skulle det med tanke på underrättelseverksamheten nödvändigt behöva föreskrivas om personbaserad underrättelseinhämtning som avser utländska förhållanden, underrättelseinhämtning som avser utländska datasystem samt underrättelseinhämtning som avser datatrafik. För de två förstnämnda typerna av underrättelseverksamhet används den gemensamma benämningen ”underrättelseinhämtning som avser utländska förhållanden”.

Det vore motiverat att göra det möjligt att använda underrättelseformer som avser utländska förhållanden också för underrättelseverksamhet inom landet. Ju närmare en verksamhet som allvarligt hotar den nationella säkerheten är, desto viktigare vore det att man får information om den och kan vidta åtgärder för att förhindra att verksamheten utvecklas i en oönskad riktning.

Med personbaserad underrättelseinhämtning avses underrättelseverksamhet som baserar sig på personliga relationer, personligt umgänge eller personlig observation av en viss person eller annat objekt. Genom att bygga upp förtroliga samarbetsrelationer med andra personer kan man med hjälp av personbaserad underrättelseinhämtning få central information om den säkerhetspolitiska miljön och om exempelvis väpnade styrkors, underrättelsetjänsters, enskilda personers eller organisationers verksamhet och om de frågor med anknytning till Finlands försvar som är föremål för deras intresse. Genom personbaserad underrättelseinhämtning kan man skaffa den information som behövs för att lämna en strategisk och operativ förvarning och skapa en lägesbild för underrättelseverksamheten.

Genom personbaserad underrättelseinhämtning kan man ta fram sådan detaljerad information som det är svårt eller omöjligt att få med andra typer av underrättelseverksamhet, och den kan också användas för att skapa förutsättningar för att effektivt utnyttja andra typer av underrättelseverksamhet.

Eftersom befogenhetsbestämmelserna bör vara exakta och väl avgränsade är det svårt att reglera befogenheterna för personbaserad underrättelseinhämtning som en enda helhet. Därför bör bestämmelser om metoderna för personbaserad underrättelseinhämtning utfärdas med beaktande av det befintliga befogenhetsregelverket. Bland de hemliga metoder för inhämtande av information som anges i 5 kap. i polislagen kan åtminstone teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, teknisk observation av utrustning, systematisk observation, förtäckt inhämtande av information, teknisk observation (teknisk avlyssning, optisk observation, teknisk spårning), inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp samt användning av informationskällor anses höra till tillämpningsområdet för den personbaserade underrättelseinhämtningen.

Med underrättelseinhämtning som avser datasystem avses underrättelseverksamhet som bedrivs med datatekniska metoder och som inriktas på uppgifter som behandlas i informationssystem.

Med underrättelseinhämtning som avser datatrafik avses underrättelseverksamhet som riktar sig mot datatrafiken i en kommunikationsnätsdel som överskrider Finlands gräns.

Bestämmelser om underrättelsebefogenheter föreslås i lagen om militär underrättelseverksamhet. Befogenheterna kallas i lagförslaget metoder för underrättelseinhämtning, och de motsvarar typmässigt och definitionsmässigt huvudsakligen de hemliga metoder för inhämtande av information som anges i 5 kap. i polislagen. Förutsättningarna för att använda metoderna för underrättelseinhämtning avviker emellertid enligt förslaget från förutsättningarna för att använda de hemliga metoderna för inhämtande av information. I fråga om vissa befogenheter krävs det preciseringar.

Eftersom bestämmelser om den militära underrättelseinhämtningens befogenheter föreslås i en särskild lag, undviker man sammanblandning med begreppen hemliga metoder för inhämtande av information eller hemliga tvångsmedel.

Därutöver föreslås i lagen bestämmelser om radiosignalspaning, platsspecifik underrättelseinhämtning, kopiering, underrättelseinhämtning som avser utländska datasystem samt underrättelseinhämtning som avser datatrafik.

2.4.4 Hemliga metoder för inhämtande av information

2.4.4.1 Förutsättningar för användning av hemliga metoder

*Allmänna och särskilda förutsättningar*

För användningen av olika metoder för informationsinhämtning har det ställts dels allmänna förutsättningar, dels särskilda förutsättningar. Särskilda förutsättningar för att använda hemliga metoder för inhämtande av information är framför allt de specificerade brott för vars förhindrande varje metod får användas. I de bestämmelser som gäller de enskilda medlem har man också kunna ställa andra särskilda villkor. Sammanfattningsvis kan man konstatera att försvarsmakten på ett heltäckande sätt får använda de hemliga metoder för inhämtande av information som det hänvisas till i lagen om militär disciplin och brottsbekämpning inom försvarsmakten på området för det militära försvaret, i syfte att förhindra brott med anknytning till olovlig underrättelseverksamhet som är straffbara enligt 12 kap. i strafflagen och högförräderibrott som är straffbara enligt 13 kap. i strafflagen.

Ovannämnda hemliga metoder för inhämtande av information får användas för att avslöja brott endast om det rör sig om äventyrande av Finlands suveränitet, krigsanstiftan, landsförräderi och grovt landsförräderi, spioneri och grovt spioneri, röjande av statshemlighet samt olovlig underrättelseverksamhet, vilka närmare regleras i 89 § 2 mom. i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. I samband med avslöjande av brott ska enligt förslaget inte tillämpas de metodrelaterade särskilda förutsättningar som avses i bestämmelserna om hemliga metoder för inhämtande av information (RP 224/2010 rd, s. 95).

Att befogenheterna graderas enligt den omfattning i vilken de ingriper ide grundläggande frioch rättigheterna kan anses vara en bra grundlösning med tanke på godtagbarheten för befogenhetsregleringen. Som förutsättningar för utövande av befogenheter kan sålunda anges ”synnerligen stor betydelse” och ”nödvändig”, vilka i 5 kap. i den gällande polislagen utgör förutsättningar för utövande av vissa befogenheter.

Underrättelseverksamhet syftar ju inte till att förhindra, avslöja eller utreda brott utan till att inhämta information om verksamhet som allvarligt hotar Finland. Utövningen av befogenheterna ska således inte kunna bindas till brott och till hur allvarliga brotten är.

I synnerhet när underrättelseinhämtningsmetoder används inom Finlands territorium bör särskild uppmärksamhet ägnas åt huruvida förutsättningar för utövande av befogenheterna föreligger. I fråga om varje befogenhet bör det fortfarande så ingående som möjligt föreskrivas om övriga förutsättningar för användningen av respektive metod, exempelvis vem befogenheten kan användas mot eller giltighetsperioden för ett tillstånd eller ett beslut.

*Brott och specificerade personer*

Ett gemensamt drag för de hemliga metoder för inhämtande av information som försvarsmakten använder är att de fastställs på basis av en viss person och en misstanke om brott. De kan bara riktas mot eller användas för att inhämta information om verksamhet som bedrivs av en person som man med fog kan anta att i framtiden kommer göra sig skyldig till ett visst brott eller som redan har gjort sig skyldig till ett visst brott eller till förberedelse för ett visst brott.

Den person som är föremål för informationsinhämtningen bör kunna individualiseras åtminstone beträffande personens roll eller uppgift, även om personens identitet ännu skulle vara okänd för de tjänstemän vid försvarsmakten som arbetar med brottsbekämpning. Med stöd av 5 kap. i polislagen får polisen rikta teleavlyssning eller teleövervakning även mot en okänd person på basis av en IP-adress eller IMEI-kod. Om en brottsbekämpningsgrund som hänför sig till en viss person saknas, kan inte försvarsmakten använda en sådan metod för informationsinhämtning enligt polislagen som det hänvisas till i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Inhämtningen av annan underrättelseinformation måste således baseras på öppna källor, radiosignalspaning, geografisk underrättelseinhämtning och sådan information som försvarsmakten via sitt samarbetsnätverk får av andra myndigheter eller av privata aktörer.

Underrättelseverksamheten kännetecknas av att man inte alltid har kännedom om en viss person, utan det primära syftet för underrättelseinhämtningen är att finna personer med anknytning till exempelvis militär verksamhet eller personer vars verksamhet utgör ett hot mot den nationella säkerheten. Därför bör man när det gäller grunderna för utövande av befogenheterna att inhämta underrättelser frångå de nuvarande kraven på misstanke om brott eller fokus på en viss person.

Medan de särskilda förutsättningarna för utövande av de nuvarande befogenheterna att inhämta information utgår från en misstanke om brott och från hur allvarliga brotten är, bör de särskilda förutsättningarna för utövande av befogenheterna att inhämta underrättelser fastställas utifrån misstänkt verksamhet och potentiellt hot. Det ska vara möjligt att i hemlighet inhämta information om verksamhet som är av militär karaktär eller som antingen direkt eller indirekt utgör ett hot mot den nationella säkerheten i Finland. Exempelvis en annan stats militära verksamhet, såsom militära övningar, uppfyller inte något brottsrekvisit och kan inte heller kriminaliseras.

Hot mot den nationella säkerheten kan vara exempelvis sådana hot som om de realiseras kan betraktas som brott men i fråga om vilka det inte ännu går att lägga fram någon konkret och specifik brottsmisstanke. Det kan också röra sig om verksamhet som inte enligt finsk lag är kriminell och som inte heller kan komma att betraktas som sådan, såsom spridning av disinformation för att den vägen påverka val.

Den verksamhet som är föremål för underrättelseinhämtning bör definieras så ingående som det överlag är möjligt.

I vårt moderna informationssamhälle accentueras samhällsfunktionernas sårbarhet och verkningarna av skador. Att man har tillgång till korrekt information och en tillförlitlig lägesbild av de hot som riktar sig mot Finlands nationella säkerhet skapar förutsättningar för att hantera hoten och fatta beslut i rätt tid. Den behöriga myndigheten ska ha det operativa ansvaret för inhämtningen av information.

Informationsinhämtningen bör omfatta kartläggning av yttre hot som riktar sig mot Finland. Det skulle således handla om att följa utvecklingen i exempelvis den militärpolitiska säkerhetsmiljön och den militära verksamheten i Finlands närområde i syfte att skapa en lägesbild. Begreppet ska också omfatta kontinuerlig informationsinhämtning om t.ex. militär verksamhet. Informationsinhämtningen ska således inte vara tidsmässigt begränsad, eftersom underrättelseverksamheten behöver bedrivas långsiktigt och vara systematisk utan att den verksamhet som är föremål för observation nödvändigtvis behöver utgöra en överhängande fara under den tid som övervakningen pågår (justitieministeriets arbetsgruppsbetänkande 41/2016, s.49).

Även om informationsinhämtningen är av långvarig art, bör det i fråga om varje metod för underrättelseinhämtning särskilt föreskrivas om tillståndets eller beslutets giltighetstid, som föreslås vara högst sex månader. När tillståndets eller beslutets giltighetstid löper ut ska det fattas ett nytt beslut om användningen av metoden i fråga, eller också ska användningen avslutas. Dessutom bör behovet av underrättelseinhämtningsmetoden och grunderna för dess användning prövas under hela den tid som metoden används och användning avslutas innan den tidsfrist som anges i beslutet har löpt ut, om syftet för användningen av metoden har nåtts eller om förutsättningar för användningen inte längre föreligger.

2.4.4.2 Metoder för inhämtning av telekommunikationsuppgifter

Tidiga informationskampanjer som riktar sig mot elektroniska kommunikationsförbindelser mellan enskilda är av central betydelse när det gäller att få sådan information om verksamhet som är föremål för militär underrättelseinhämtning som gör det möjligt att skapa en adekvat lägesbild och vidta åtgärder för att avvärja hot. Det relevanta är att dels få information om innehållet i den elektroniska kommunikationen, dels annan information om kommunikationen, exempelvis förmedlingsuppgifter. Utifrån innehållet i kommunikationen kan man skapa en mer konkret bild av föremålet för den militära underrättelseinhämtningen och få mer detaljerad information om verksamheten. Förmedlingsuppgifter åter är nödvändiga för att identifiera de personer som deltar i verksamheten.

Teleavlyssning och teleövervakning kan endast riktas mot en sådan teleadress eller teleterminalutrustning som med viss säkerhet är i en viss persons besittning eller användning. I beslutet om teleavlyssning och teleövervakning ska också den personen nämnas, även om personens identitet kan vara okänd. Ingendera metoden för inhämtande av information får riktas enbart mot en person utan att teleadressen eller teleterminalutrustningen har identifierats, utan ett separat tillstånd ska sökas för varje teleadress och teleterminalutrustning. Detta är problematiskt med hänsyn till hur underrättelseverksamhet till sin karaktär avviker från brottsbekämpning – underrättelseverksamheten har särdrag som gör att man måste kunna arbeta med bredare kriterier när man riktar verksamheten.

Det är mycket lätt att teckna förbetalda abonnemang och andra anonyma abonnemang, och den tekniska utvecklingen har också gjort att sådana är billiga att köpa och använda. En person kan förfoga över tiotals anonyma abonnemang och teleterminalutrustningar, exempelvis mobiltelefoner. I många fall försvårar detta teleavlyssning och teleövervakning, och dessa metoder blir också mindre effektiva som hemliga metoder för inhämtning av information. Dessu-

tom medför de onödiga personkostnader för myndigheterna, domstolsväsendet och teleföretagen.

Det är befogat att den reglering som gäller riktande av teleavlyssning och teleövervakning i underrättelsesyfte utvidgas till att också gälla enskilda personer. Teleavlyssning skulle därmed riktas endast mot meddelanden från eller meddelanden avsedda för en viss person, medan det i fråga om nya teleabonnemang eller ny teleterminalutrustning som påträffas hos den personen inte skulle krävas flera nya tillstånd så länge det personbaserade tillståndet är i kraft. På så sätt slipper man fatta flera olika tillståndsbeslut som gäller samma person. Detta bidrar också till att förbättra säkerheten för aktörerna inom tillståndsprocessen.

Den ovan beskrivna regleringen av metoderna för inhämtning av telekommunikationsuppgifter påverkar hur teleavlyssning och teleövervakning genomförs rent tekniskt. Teleavlyssning och teleövervakning genomförs möjligast nära den teleadress eller terminalutrustning som är föremål för informationsinhämtningen, dvs. vid en punkt där ingen annan kommunikation passerar än den som utgår från eller kommer till den adress eller terminalutrustning som är föremål för informationsinhämtningen. Nättopologiskt sett, dvs. med avseende på kommunikationsnätets logiska struktur, sker teleavlyssning och teleövervakning i kommunikationsnätets periferi.

Metoder för inhämtning av telekommunikationsuppgifter kan inte användas om man inte har uppgift om de enskilda teleadresser eller teleterminalutrustningar som används i kommunikationen i den verksamhet som är föremål för informationsinhämtning. I sådana situationer kan man inte använda de metoderna ens i det fallet att man har information eller misstanke om ett brott som kan utgöra grund för teleavlyssning eller teleövervakning och om fakta i fallet. Metoderna för inhämtning av telekommunikationsuppgifter gör det inte möjligt att inhämta information om de kommunikationsmedel eller kommunikationskanaler som används i den verksamhet som är föremål för informationsinhämtningen, eftersom en lagstadgad förutsättning för att metoder för informationsinhämtning ska få användas och genomföras tekniskt är att man redan har kännedom om kommunikationsmedlen eller kommunikationskanalerna.

Om försvarsmakten har information om en person som med fog kan antas göra sig skyldig till ett brott som utgör grund för teleavlyssning eller teleövervakning men saknar information om enskilda teleadresser eller teleterminalutrustning som den personen använder, kan identifieringsuppgifter för teleadresser eller teleterminalutrustning ofta inhämtas med hjälp av de befogenheter som gäller dem. Den tekniska utrustning som används för verksamheten bör vara sådan att den inte kan användas för andra ändamål än för att identifiera teleadressen eller teleterminalutrustningen. Befogenheten att inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning gör det möjligt att i ett senare skede rikta teleavlyssning eller teleövervakning mot adressen eller terminalutrustningen, om förutsättningarna för att använda dessa informationsinhämtningsmetoder uppfylls.

De nuvarande metoderna för inhämtning av telekommunikationsuppgifter lämpar sig endast för att inhämta information om sådana brott som man redan med viss säkerhet känner till, som motsvarar ett visst brottsrekvisit och som antingen är under beredning eller som sannolikt har begåtts, där de involverade personerna och de identifierade teleadresser och teleterminalutrustning som de använder redan är kända när informationsinhämtningen inleds. Ur underrättelsesynvinkel är de hemliga metoder för inhämtande av telekommunikationsuppgifter som anges i polislagen inte lämpliga för att upptäcka och identifiera hot. Detta beror på karaktären av dessa metoder och deras tekniska genomförande.

Teleavlyssning är en bristfällig metod när det gäller att upptäcka och identifiera föremål för militär underrättelseinhämtning. Detta påverkas inte på något avgörande sätt av exempelvis huruvida teleavlyssning och teleövervakning såsom för närvarande används för att förhindra brott eller huruvida dessa metoder också kan användas som metoder för underrättelseinhämtning för att skaffa information om militär verksamhet eller om hot mot den nationella säkerheten. Även om man utfärdar bestämmelser om teleavlyssning och teleövervakning som företas i underrättelsesyfte kommer detta inte nämnvärt att öka förmågan att upptäcka och identifiera okända hot som riktar sig mot det finska samhällets centrala säkerhetsintressen eller personerna bakom hoten, eftersom en uttrycklig förutsättning för att dessa metoder ska få användas också för underrättelsesyften ska vara att man har kännedom om föremålet för den militära underrättelseinhämtningen, de bakomliggande personerna och de konkreta kommunikationsmedel de använder redan då teleavlyssningen eller teleövervakningen inleds. En annan sak är att bestämmelser om teleavlyssning och teleövervakning som företas i underrättelsesyfte kan bedömas väsentligt förbättra tillgången till information om sådan verksamhet som är föremål för militär underrättelseinhämtning som inte är brottslig verksamhet eller som inte ännu har utvecklats till en konkret och specifik misstanke om brott. Till denna del skulle det röra sig om en utvidgning av den materiella räckvidden för metoderna för inhämtning av telekommunikationsuppgifter som dock inte i grunden förändrar metodernas karaktär.

Detsamma kan konstateras i fråga om utvidgningen av den materiella räckvidden för metoderna för inhämtning av telekommunikationsuppgifter genom kriminalisering av sådana former av verksamhet som är föremål för militär underrättelseinhämtning som för närvarande inte är straffbara. Att man breddar spektrumet av gärningar som kan utgöra en grund och särskild förutsättning för användning av metoder för inhämtning av telekommunikationsuppgifter kommer inte att förändra den grundläggande karaktären av dessa informationsinhämtningsmetoder.

De säkerhetshot som hör till försvarsmaktens ansvarsområde kan vara sådana att hoten och de bakomliggande personerna vistas i olika länder. Den elektroniska kommunikationen mellan dem är därmed gränsöverskridande. Bristerna i de metoder för inhämtning av telekommunikationsuppgifter som anges i 5 kap. i polislagen accentueras ofta i sådana fall där man behöver få information om kommunikation mellan Finland och något annat land. Ofta rör det sig om situationer där den part i kommunikationen som är i utlandet – exempelvis en representant för en främmande stats väpnade styrkor eller underrättelse- och säkerhetstjänst – som en följd av internationellt informationsutbyte kan identifieras med en viss grad av exakthet, medan den part som finns i Finland är okänd. Det kan t.ex. vara fråga om att man vet eller misstänker att en främmande stats väpnade styrkor kommunicerar med en person i Finland eller styr samarbetsparter som är utsända i Finland eller i övrigt vistas här, eller om att man har fått information om att en främmande stats underrättelsetjänst har sänt ut underrättelseofficerare som arbetar under täckmantel i Finland. Om man inte känner till vilka personer i Finland som deltar i verksamheten eller vilka kommunikationsmedel de använder, kan man inte rikta inhämtningen av telekommunikationsuppgifter mot den gränsöverskridande kommunikationen ens i det fall att man känner till kommunikationsparten i utlandet. Med andra ord kan man inte använda de nuvarande metoderna för inhämtning av telekommunikationsuppgifter för att upptäcka eller identifiera personer som vistas i Finland och som är delaktiga i gränsöverskridande verksamhet som är föremål för militär underrättelseinhämtning, trots att en förutsättning för att man ska få mer exakt information om sådan verksamhet och i sista hand kunna avvärja hot skulle vara att man kan upptäcka och identifiera sådana personer. Detta är en avsevärd brist i en situation där Finlands säkerhetspolitiska miljö har försämrats och sannolikt ytterligare kommer att försämras på nästan alla delområden.

Definitionen av teleavlyssning täcker sådana situationer där ett meddelande överförs över ett allmänt kommunikationsnät. Teleavlyssning kan inte riktas mot ett meddelande som inte ännu har nått det allmänna kommunikationsnätet. Begreppet allmänt kommunikationsnät täcker inte heller särskilda situationer som exempelvis satellittelefonnät eller andra kommunikationsformer som eventuellt kommer att utvecklas i framtiden.

I dess nuvarande form kan teleavlyssning inte anses vara användbar för underrättelseverksamhet som sker i utlandet. Eftersom man kan utgå från att den som äger det allmänna kommunikationsnätet i en främmande stat sannolikt inte är villig att göra de kopplingar i det allmänna kommunikationsnätet som krävs för teleavlyssning, kan definitionen av teleavlyssning inte anses täcka dessa situationer. Till dessa delar borde därför användningsområdet för teleavlyssningen utvidgas till att omfatta ovan avsedda situationer.

2.4.4.3 Observationsbaserade metoder för informationsinhämtning

I 89 § 1 mom. i lagen om militär disciplin och brottsbekämpning inom försvarsmakten hänvisas det i fråga om den systematiska observation som används vid brottsbekämpning inom försvarsmakten till 5 kap. 13 § i polislagen. Definitionen av observation i 5 kap. 13 § 1 mom. i polislagen har instrumentell betydelse i fråga om flera hemliga metoder för inhämtande av information, i synnerhet med hänsyn till bestämmelserna om teknisk observation. För tillfällig observation krävs ingen befogenhetsreglering. Situationen blir en annan när den misstänkte observeras annat än kortvarigt. Då handlar det om inhämtning av information som ska anses vara systematisk, där den misstänktes liv övervakas under en viss tid. En sådan observation ingriper i integritetsskyddet för den person som är föremål för observationen, eftersom man övervakar vad den berörda personen gör under sin fritid och vem den träffar. På grund av den systematiska observationens karaktär och behovet av heltäckande reglering av myndighetsbefogenheterna bör bestämmelser om sådan observation utfärdas i lag.

I fråga om den observation som sker i internet är den rådande uppfattningen den att det inte behövs någon särskild befogenhetsreglering vid observation som sker i allmänna datanät, exempelvis på ett diskussionsforum. Här föreslås det inga ändringar. Den observation som sker i datanäten bör liksom annan observation vara passiv inhämtning av information som avser interaktionen mellan människor. Enbart observation av en viss byggnad, ett visst utrymme, en viss plats, ett visst diskussionsforum eller något motsvarande objekt ska inte anses innebära att observationsbefogenheten används. Det är inte nödvändigt att i lag föreskriva om att sådan observation är tillåten.

Vid systematisk observation får man använda kikare, kamera, videokamera, bildförstärkare eller andra motsvarande tekniska anordningar som också för närvarande får användas vid observation. Användningen av sådana anordningar ändrar inte åtgärdens karaktär: den är densamma som vid iakttagelser som grundar sig enbart på sinnesförnimmelser. Gränsdragningen mot optisk observation skulle bestå i att man vid optisk observation använder tekniska anordningar, tekniska metoder och programvara som placeras ut på en viss plats.

Bakom de hot mot försvaret och de allvarliga säkerhetshot som hör till försvarsmaktens ansvarsområde ligger ofta organiserad verksamhet där man inte alla gånger kan identifiera enskilda personer. Involverade personer kan vara omedvetna om att de deltar i verksamhet som utgör ett hot mot försvaret eller den nationella säkerheten. I en sådan situation vore det ytterst viktigt att kunna observera verksamheten som en helhet, trots att man inte ännu kan eller behöver identifiera enskilda personer och trots att ingen förefaller göra sig skyldig till brott. För närvarande kan systematisk observation endast riktas mot personer.

Försvarsmaktens nuvarande metoder att inhämta information genom observation lämpar sig endast för att få information om sådana brott som man redan med viss säkerhet känner till, som motsvarar ett visst brottsrekvisit och som antingen är under beredning eller som sannolikt har begåtts, där den involverade personen redan är känd när myndigheten inleder informationsinhämtningen.

Under de nuvarande förutsättningarna lämpar sig observation inte för att upptäcka hot. Däremot kunde observation användas som metod för underrättelseinhämtning. Därför är det viktigt att se till att observation är ett alternativ också när det gäller att inhämta information om verksamhet som är av militär karaktär eller som allvarligt hotar den nationella säkerheten.

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 tjänstemans uppdrag. Eftersom befogenheten endast används kortvarigt, placerar sig förtäckt inhämtande av information som metod i gränsområdet mellan systematisk observation och täckoperationer. Metoden har klart gemensamma drag med täckoperationsverksamhet. Vid förtäckt inhämtande av information uppstår emellertid inte samma förtroenderelation mellan aktören och objektet. Täckoperationer kan för närvarande utifrån misstanke om brott riktas mot en viss person, som inte behöver vara den person som antas göra sig skyldig till brott. I underrättelseverksamhet bör också en grupp av personer kunna utgöra föremål för förtäckt inhämtande av information, även om det egentliga umgänget och personkontakterna i operationellt hänseende skulle gälla enskilda personer inom gruppen.

Gemensamt för de hemliga metoder för inhämtande av information som ingår i teknisk observation är att användningen av dessa metoder förutsätter att man specificerar en viss person, ett visst utrymme eller område eller någon annan plats. Gemensamt för de befogenheter som gäller teknisk observation är att de innebär att avlyssningen, observationen eller övervakningen sker utan att observatören är närvarande vid situationen eller befinner sig i dess omedelbara närhet. Teknisk observation kan genomföras teknikneutralt med en teknisk anordning eller metod eller med hjälp av programvara. Vid utövandet av befogenheterna för teknisk observation kan man således förutom att ansluta en extern anordning till ett visst föremål eller installera en extern datateknisk applikation i ett föremål även utnyttja föremålets befintliga egenskaper, exempelvis lokaliseringsteknik, mikrofon eller kamera som finns i föremålet.

Teknisk avlyssning och optisk observation bör granskas med hänsyn till vissa bestämmelser i strafflagen. Olovlig avlyssning kriminaliseras i 24 kap. 5 § 1 mom. i strafflagen och olovlig observation i strafflagens 24 kap. 6 §. Dessa bestämmelser i strafflagen har uttryckligen lämnats utanför bestämmelserna om befogenheter för teknisk avlyssning och optisk observation, för att det inte ska uppstå ovisshet om deras tillämpning i fråga om teknisk avlyssning och optisk observation. För att ovannämnda kriminaliseringar inte ska bli tillämpliga bör förutsättningarna att utöva befogenheterna uppfyllas.

Det primära syftet med optisk observation är att ta fram sådant bildmaterial som vid behov kan användas exempelvis för att analysera information eller som kan ha betydelse i sig självt. I vissa fall kan man pruta på bildkvaliteten, exempelvis när man enbart behöver information om personers eller gruppers rörelser på ett visst område. Optisk observation kan ersätta en stor del av de årsverken som annars skulle behövas. Som exempel kan nämnas situationer där en eller flera byggnader eller områden behöver övervakas dygnet runt, och försvarsmaktens tjänstemän inte kan genomföra observationen på grund av särskilda omständigheter som gäller övervakningsobjektet.

Inom den militära underrättelseinhämtningen vore det väsentligt att man får så aktuell och specificerad information som möjligt om innehållet i en kommunikation. Teknisk avlyssning gör det möjligt att inhämta heltäckande och detaljerad information om en viss verksamhet och om personer och grupper av personer som har samband med verksamheten. Syftet med den tekniska avlyssningen är såväl att identifiera den utpekade personen eller gruppen av personer som att inhämta information om deras verksamhet.

Övervakning av personers och gruppers rörelser och av transporter (av föremål, ämnen eller egendom) genom teknisk övervakning ger försvarsmakten möjlighet att planera och rikta in åtgärder. Annan teknisk spårning än teknisk spårning av en person avviker från optisk observation och teknisk avlyssning i synnerhet genom att den inte lika kraftigt ingriper i de grundläggande fri- och rättigheterna och mänskliga rättigheterna. Genom ändamålsenlig användning av teknisk spårning kan man komplettera den observation som normalt används inom den militära underrättelseinhämtningen. Det är emellertid skäl att påpeka att teknisk spårning i likhet med optisk observation och teknisk avlyssning inte i alla situationen helt kan ersätta tjänstemannens egna iakttagelser. Teknisk spårning av en person däremot innebär ingrepp i de grundläggande fri- och rättigheterna och mänskliga rättigheterna, exempelvis den fria rörligheten och skyddet för privatlivet.

Av underrättelseverksamhetens karaktär följer att de befogenheter som utövas utövas i hemlighet för den som är föremål för underrättelseinhämtningen. Teknisk observation av utrustning gör det möjligt att rikta underrättelseinhämtningen mot exempelvis dokument som finns i en dator. Teknisk observation av utrustning är en nödvändig befogenhet exempelvis i samband med platsspecifik underrättelseinhämtning, om man behöver inhämta information i digital form ur dokument som finns i en teknisk anordning.

I fråga om teknisk observation av utrustning bör det beaktas att definitionen av teknisk observation av utrustning i polislagens 5 kap. inte i nuläget gör det möjligt att inhämta information om innehållet i ett meddelande. Detta innebär att ett meddelande som lagrats i en viss anordning inte kan klarläggas genom teknisk observation av utrustning och inte heller med de övriga befogenheter som anges i polislagens 5 kap. Genom teknisk observation av utrustning kan man t.ex. ta del av innehållet i ett meddelande i det ögonblick som meddelandet skrivs, och genom teleavlyssning kan man ta del av innehållet i ett meddelande när det förmedlas i ett allmänt kommunikationsnät.

Bestämmelserna om de befogenheter som kan användas inom den militära underrättelseinhämtningen bör kunna svara på utmaningarna från den tekniska utvecklingen i omvärlden, vilket också bör beaktas vid bedömningen av den gällande lagstiftningens funktionsduglighet. Detta gäller såväl de metoder som används som den verksamhet som är föremål för underrättelseinhämtningen.

Bestämmelser om befogenhet att inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning behövs också i fråga om militär underrättelseinhämtning. Metoden kan användas för att inhämta information som gör det möjligt att rikta befogenheter som ingriper i skyddet för hemligheten i fråga om förtroliga meddelanden (teleavlyssning och teleövervakning) mot ett föremål för militär underrättelseinhämtning. Metoden kan därmed bidra till att förbättra skyddet för utomstående personers grundläggande fri- och rättigheter.

I nuläget får man för att inhämta identifieringsuppgifter använda en anordning som endast kan användas för att inhämta ifrågavarande uppgifter. Eftersom anordningen till sina tekniska

egenskaper är sådan att den också lämpar sig för annan verksamhet, vore det ändamålsenligt att användningsändamålet för anordningen utvidgas.

Bestämmelsen om installation och avinstallation av anordningar, metoder eller programvara är framför allt en bestämmelse som möjliggör teknisk observation. I praktiken skulle det ofta vara omöjligt eller åtminstone ytterst svårt att genomföra teknisk observation utan en sådan befogenhet.

Försvarsmaktens nuvarande metoder för att inhämta information genom observation lämpar sig för att inhämta information endast om sådana brott som man redan med viss säkerhet känner till, som motsvarar ett visst brottsrekvisit och som antingen är under beredning eller som sannolikt har begåtts, där den involverade personen redan är känd när myndigheten inleder informationsinhämtningen. För närvarande lämpar sig teknisk observation inte för att upptäcka och identifiera hot.

Eftersom de ovan beskrivna observationsbaserade metoderna för informationsinhämtning är effektiva och i relativt liten utsträckning ingriper i de grundläggande fri- och rättigheterna kommer de att ha en viktig roll som metoder för militär underrättelseinhämtning. Genom att på rätt sätt och i ett så tidigt skede som möjligt inrikta de befogenheter som används inom den militära underrättelseinhämtningen kan man minska kretsen av personer som underrättelseverksamheten riktar sig mot.

Den information i realtid som man får med hjälp av de observationsbaserade metoderna kan betydligt förbättra lägesbilden och därmed göra det lättare att fatta beslut om inriktningen av och prioriteringarna inom den militära underrättelseinhämtningen. Med den information man får kan man öka den militära underrättelseinhämtningens genomslag.

När befogenheter utövas i underrättelsesyfte rör det sig inte om åtgärder som syftar till att förhindra, avslöja eller utreda brott. Vid militär underrättelseinhämtning medför identifieringen av en viss person därmed inte ett motsvarande behov att bedöma de särskilda förutsättningarna för användning av befogenheten, såsom huruvida det finns anledning att misstänka personen i fråga för ett brott som överstiger gränsen för ett visst straffhot eller om personen kan antas göra sig skyldig till ett sådant brott. Trösklarna för att utöva befogenheterna annat än på basis av misstanke om brott bör emellertid anpassas utifrån underrättelseverksamhetens karaktär.

Användningssyftet för de befogenheter som utövas i underrättelseinhämtningen kan vara t.ex. att inhämta information om organisationen för en viss grupp av personer, om de personer som hör till gruppen och om gruppens aktivitet inom ett visst område samt om formerna för gruppens verksamhet. Sådan information kan ha betydelse för såväl det operativa som det strategiska beslutsfattandet. Bland annat av ovannämnda orsaker bör också de observationsbaserade befogenheterna kunna riktas mot en avgränsad grupp personer.

2.4.4.4 Täckoperationer och bevisprovokation genom köp

För närvarande ska de som utsätts för en täckoperation kunna individualiseras åtminstone utifrån sina uppgifter med anknytning till brottslig verksamhet. Detta förutsätter inte att personerna namnges. Inom den militära underrättelseinhämtningen bör täckoperationer kunna riktas också mot en viss grupp av personer, där inte samtliga enskilda personer som bildar gruppen utsätts för täckoperationen. I en del fall behöver information inte inhämtas om en enskild persons verksamhet, i stället behöver det vara möjligt att infiltrera t.ex. en viss grupp av människor för att den vägen inhämta information om den bakgrundsorganisation som styr gruppens

verksamhet och om personerna i organisationen. Det kan vara fråga om t.ex. hybridpåverkan på förhållandena i Finland.

Täckoperationer och bevisprovokation genom köp anses vara de mest drastiska hemliga metoderna för inhämtande av information, vilket är anledningen till att förutsättningarna för att använda dem är mycket strikta. För att täckoperationer och bevisprovokation genom köp ska få användas förutsätts att det är nödvändigt för att förhindra eller avslöja brott. En ytterligare förutsättning som gäller täckoperationer är 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. Det är befogat att föreskriva om lika strikta förutsättningar för täckoperationer och bevisprovokation genom köp också i samband med användning av dem som metoder för underrättelseinhämtning inom militär underrättelseverksamhet, fastän syftet med dem inte är att inhämta brottsrelaterad information.

I 5 kap. 29 § i polislagen föreskrivs det om brottsförbud. I strid med paragrafrubriken innefattar brottsförbudet rätt för en polisman som företar en täckoperation att begå lindriga förseelser. I 5 kap. 30 § i polislagen föreskrivs det 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 med dessa 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 sistnämnda bestämmelsen kan en polisman som företar en täckoperation under sitt deltagande i en organiserad kriminell sammanslutnings verksamhet med andra ord delvis begå straffbara handlingar som uppräknas i 17 kap. 1 a § i strafflagen. I paragrafen om befogenheter nämns inte dessa straffbestämmelser, men det kan också bli fråga om att befrias från ansvar för medverkan till brott.

Täckoperationer och bevisprovokation genom köp är metoder som redan nu i första hand anses vara av underrättelsetyp, inte nödvändigtvis en del av förundersökningen. Också människorättsdomstolen har uppfattat polisens okonventionella metoder för inhämtande av information uttryckligen som underrättelseverksamhet, och de bedöms enligt kriterier som till en del skiljer sig från de kriterier som gäller förfarandet för rättegång i brottmål eller det förundersökningsförfarande som är en del av det. När dessa metoder bedöms med tanke på militär underrättelseinhämtning anläggs ett perspektiv som är ännu mer fjärran från brottsbegreppet, eller så kommer brottsrelaterad användning inte alls på fråga.

Täckoperationer möjliggör erhållande av detaljerad information om den verksamhet som underrättelseinhämtningen riktas mot. Dessutom har Försvarsmakten kännedom om sitt verksamhetsfält och kompetens som hänför sig till det, därför kan det anses att Försvarsmakten är den enda myndigheten med know-how när det gäller att verka inom en militärorganisation också under täckoperationer.

Eftersom det inom underrättelseverksamheten kan vara ändamålsenligt att företa täckoperationer för att delta i verksamhet som går ut på att planera aktioner som riktas mot Finland gäller det att ändra också strafflagen för dessa situationers vidkommande.

*Att skydda täckoperationer och bevisprovokation genom köp*

Den ståndpunkt som förvaltningsutskottet i tiderna (FvUB 17/2000) intog, nämligen att bevisprovokation genom köp i princip ska hemlighållas strikt, motsvarar det synsätt som förundersökningsmyndigheterna i dag företräder. Sedan dess har utskottets ställningstagande till bevisprovokation genom köp anammats principiellt, åtminstone inom polisverksamheten. Enligt förvaltningsutskottet räcker det ibland med blotta vetskapen om att en täckoperation eller bevisprovokation genom köp har använts för att verksamheten ska avslöjas i minsta detalj. Enligt förvaltningsutskottet äventyras inte den åtalades rätt till en rättvis rättegång om information som inhämtats genom täckoperation eller bevisprovokation genom köp inte har använts som grund för åtalsprövningen eller under rättegången utan endast har hjälpt polisen att fokusera sina aktioner.

Den nämnda utgångspunkten visar att det finns en viktig principiell skillnad mellan bevisprovokation genom köp och täckoperationer å ena sidan och det straffprocessuella rättsliga systemet som bygger på legalitetsprincipen å andra sidan. En motsvarande spänning kan inte anses ingå i sådana täckoperationer och sådan bevisprovokation genom köp som används på underrättelsebasis och där det primära syftet inte är att inhämta information med tanke på straffprocessen eller för något annat ändamål än inriktande av den militära underrättelseverksamheten. Trots denna grundval som gäller användningsförutsättningarna är det nödvändigt av säkerhetsskäl och för att underrättelseoperationerna ska vara framgångsrika att utförandet av bevisprovokation genom köp och täckoperationer hemlighålls strikt. Om bevisprovokation genom köp avslöjas kan följden vara att en person som uppträtt under täckmantel blir utsatt för hot mot liv eller hälsa i form av hot om hämndåtgärder. Hämndåtgärder kan också rikta sig mot personens närstående och mot utomstående som eventuellt har försett personen med information eller på annat sätt främjat underrättelseverksamheten. Hemlighållandet av bevisprovokation genom köp och täckoperationer är förståeligt också från den synpunkten att om åtgärder av det slaget alltid skulle tillkännages för dem som de riktar sig mot skulle det kunna bli omöjligt att använda dessa metoder för underrättelseinhämtning.

*Övervakning*

Kontrollen av hur förfarandereglerna för täckoperationer och bevisprovokation genom köp iakttas sköts i praktiken ofta internt. Det är viktigt att man i realiteten är kapabel att effektivt övervaka täckoperationer och bevisprovokation genom köp också när dessa metoder används inom underrättelseverksamhet.

De övervakningsstrukturer som gäller täckoperationer och bevisprovokation genom köp bör vara färdiga innan verksamheten inleds. Förutom den interna övervakningen och den övervakning som försvarsministeriet utför kommer underrättelseombudsmannen, som är en oberoende rättslig övervakare, att spela en framträdande roll vid övervakningen av täckoperationer och bevisprovokation genom köp, alldeles som vid övervakningen av andra metoder för underrättelseinhämtning.

2.4.4.5 Styrd användning av informationskällor och tryggande av informationskällornas säkerhet

Eftersom Försvarsmakten och militärunderrättelsemyndigheterna har kompetens och know-how vad den militära verksamhetsmiljön beträffar kan det anses att endast de har tillräcklig kompetens för att identifiera parter och organisationer som är av mycket stor betydelse för den militära underrättelseinhämtningen och centrala personer som skulle kunna fungera som informationskällor.

Den nuvarande regleringen gör det möjligt att hemlighålla kontakter mellan informationskällor och tjänstemän som inhämtar information. Bestämmelser om detta finns närmast i 5 kap. 46 § i polislagen, där det föreskrivs om skyddande av hemligt inhämtande av information. Med stöd av paragrafen kan en informationskälla emellertid inte t.ex. ges en ny identitet, utan avsikten är att skydda verksamheten och även informationskällan via de tjänstemän som utför arbetet i fråga. Därmed kan enbart tjänstemän bli delaktiga av det skydd som avses i paragrafen, och bara de kan använda skyddet.

En myndighet som använder en informationskälla är i princip skyldig att trygga informationskällans säkerhet efter behov under och efter informationsinhämtningen. Det finns emellertid ingen reglering om förebyggande skydd av informationskällor. De informationskällor som används inom underrättelseverksamheten kan i en del fall försätta sig i situationer där deras liv och hälsa hotas, varvid hotet kan komma från statligt håll. Det kan vara fråga om t.ex. en ansökan om politisk asyl. I sådana fall förutsätter skyddet av informationskällan en annan intensitet än den som avses i de bestämmelser i 5 kap. i polislagen som gäller användning av informationskällor. Militärunderrättelsemyndigheten bör vara kapabel att skydda en potentiell informationskälla redan i förväg för att informationskällan ska kunna lita på att hen får adekvat skydd. Vid långvarigare skyddsbehov och som yttersta medel bör man överväga ett vittnesskyddsprogram enligt lagen om vittnesskyddsprogram (88/2015). Med anledning av det som sägs ovan behöver det föreskrivas om tryggande av informationskällans säkerhet på ett sådant sätt att tryggandet kan inledas i förebyggande syfte.

2.4.4.6 Genomsökning

Varken lagen om militär disciplin och brottsbekämpning inom försvarsmakten eller polislagen upptar för närvarande bestämmelser om platsgenomsökning i informationsinhämtningssyfte. I 8 kap. i tvångsmedelslagen (806/2011) föreskrivs det däremot om platsgenomsökning för utredning av begångna brott. Genomsökningar som utförs enligt den gällande tvångsmedelslagen har till syfte att inhämta bevis för brott, och personen i fråga ska vara närvarande eller ha kännedom om genomsökningen. Man bör emellertid lägga märke till att det i tvångsmedelslagen för tillfället inte finns några bestämmelser om genomsökning i informationsinhämtningssyfte där den som genomsökningen riktas mot inte är medveten om genomsökningen, därför har termen ”genomsökning” i denna proposition inte samma innebörd som genomsökning enligt den gällande tvångsmedelslagen.

Inom underrättelseverksamheten förekommer situationer där det är nödvändigt att utföra genomsökning av platser för att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten. Hur länge inhämtningsskedet pågår kan inte bestämmas i förväg utan beror på arten av och beskaffenheten hos den information som Försvarsmakten inhämtar när den utövar sina lagstadgade befogenheter. Om den som är föremål för militärunderrättelsemyndighetens informationsinhämtningsåtgärd upptäcker åtgärden äventyras fullgörandet av informationsinhämtningens syfte, vilket kan medföra fara för liv eller hälsa för berörda tjänsteman vid militärunderrättelsemyndigheten.

Samhällsintresset är desto större ju allvarligare förehavandet eller fenomenet i fråga är. Utgångspunkten är att all verksamhet som allvarligt hotar den nationella säkerheten är sådan på grund av sin skadlighet att informationsinhämtning i så stor skala som möjligt bör kunna genomföras.

Exempelvis är en främmande makts förberedelser för militära aktiviteter på en annan stats territorium planmässiga, systematiskt målinriktade och kollektiva. En konsekvens av det kollektiva inslaget är att delåtgärder som är nödvändiga för att möjliggöra sådana förehavanden fördelas mellan olika parter. Då kan det visa sig vara en ytterst stor utmaning att inhämta information om verksamheten som helhet. Med hjälp av organisationsformer som är uppbyggda av celler eller i form av nätverk minimeras gruppens synlighet och hemlighålls planerna så effektivt som möjligt. Ofta förekommer bara ett minimum av kontakter mellan medlemmarna i gruppen, eller så görs det så svårt som möjligt för utomstående att uttolka innehållet i kommunikationen. De tekniska krypteringsmöjligheter och det anonymitetsskydd som den moderna kommunikationstekniken står till tjänst med utnyttjas effektivt. Alla de ovannämnda faktorerna bidrar till att Försvarsmaktens metoder för informationsinhämtning inte alltid resulterar i sådan information med vars hjälp landets försvar skulle kunna tryggas.

Trots det som sägs ovan är det ett faktum att en främmande makts militära aktiviteter och påverkansverksamhet av annat slag som riktas mot Finland förutsätter att fysiska åtgärder vidtas i den reella världen. Åtgärder av det slaget brukar lämna spår av olika slag och intensitet. Spåren kan vara t.ex. utkast, dokument där gruppens interna arbetsfördelning framkommer, anteckningar om rekognoscering eller övervakning som gäller det tilltänkta objektet, resedokument, e-postmeddelanden om genomförande av planen som öppnats med hjälp av ett krypteringsprogram, eller ämnen eller föremål som behövs för att genomföra planen. I vissa fall kan information om ovannämnda eller liknande omständigheter fås med hjälp av genomsökning av t.ex. ett utrymme som en person eller grupp använder för sina möten eller som förråd. Genomsökningen kan resultera i information som kan antas vara mycket viktig och handlar om militära aktiviteter eller verksamhet som allvarligt hotar den nationella säkerheten.

Det är inte motiverat att underrätta den som åtgärden riktas mot om en sådan genomsökning, eftersom det kan vara nödvändigt att fortsätta att inhämta information om hens verksamhet ännu efter att genomsökningen utförts. En sådan skyldighet att underrätta personen i fråga som är knuten till tidpunkten för utförande av genomsökningen skulle omöjliggöra framtida framgångsrik informationsinhämtning. Detta kan bero t.ex. på att genomsökningen utförts vid fel tillfälle. Man kan tänka sig en situation där militärunderrättelsemyndigheten får som tillförlitlig betraktad information om att en okänd person ska träffa den som är föremål för informationsinhämtningen och ge hen en viktig plan. Militärunderrättelsemyndigheten har då kännedom om leveransen men inte om den exakta tidpunkten för den. Om militärunderrättelsemyndigheten före denna träff genomsöker ett utrymme som personen i fråga har i sin besittning, utgör en underrättelse till personen om genomsökningen en varning som får hen att ändra sin handlingsplan. För att helhetsbilden ska kunna säkerställas kan det bli nödvändigt att utföra en samtidig genomsökning av flera objekt, varvid uppgifter om genomsökningen inte får nå eventuella andra kumpaner.

För att informationsinhämtningen ska vara effektiv gäller det därmed att personen i fråga åtminstone inte direkt blir medveten om de åtgärder som riktas mot hen. Det är snarare fråga om hemligt inhämtande av information än om genomsökning som det föreskrivs om i tvångsmedelslagen. I regel bör personen ändå underrättas om åtgärderna i ett senare skede. Underrättelsen ska lämnas efter att syftet med informationsinhämtningen har nåtts. Det föreslås ändå att skyldigheten att göra underrättelsen kan skjutas upp eller underrättelsen får utebli, om synner-

ligen viktiga intressen från fall till fall talar för detta. Det är motiverat att förutsättningarna för att skjuta upp eller frångå underrättelseskyldigheten är på samma nivå som beträffande de hemliga metoderna för inhämtande av information enligt 5 kap. i polislagen. Genomsökning skulle kunna benämnas platsspecifik underrättelseinhämtning.

2.4.4.7 Kopiering

Inom den militära underrättelseinhämtningen är det nödvändigt att dokumentera iakttagelser och fynd medan platsspecifik underrättelseinhämtning pågår samt även i övrigt. Utgångspunkten är att det bör vara möjligt att kopiera ett föremål, egendom, dokument, information eller en omständighet som påträffats vid platsspecifik underrättelseinhämtning. Med tanke på genomförandet av platsspecifik underrättelseinhämtning behöver det i 4 kap. i lagen om militär underrättelseverksamhet föreskrivas om kopiering som en metod för underrättelseinhämtning på ett sätt som vad metodiken beträffar motsvarar det som i tvångsmedelslagen föreskrivs om kopiering. Anteckningar om kopieringen ska göras i ett protokoll över den platsspecifika underrättelseinhämtningen, och dessutom ska ett separat protokoll upprättas över varje kopiering. Vidare ska den som åtgärden riktas mot eller den vars egendom, föremål eller dokument det är fråga om underrättas om kopieringen på samma sätt som om användning av metoder för underrättelseinhämtning.

Eftersom utgångspunkten är att det är meningen att den militära underrättelseverksamheten och de metoder för underrättelseinhämtning som används i samband med den ska hemlighållas för den som är föremål för åtgärder kommer det inte på fråga att omhänderta dokument, föremål eller egendom som tillhör hen. Därför är kopiering nödvändig för att det ska vara möjligt att undvika uppteckning av iakttagelser och fynd och för att risken att t.ex. platsspecifik underrättelseinhämtning avslöjas samtidigt ska minimeras. Om det i samband med militär underrättelseinhämtning, t.ex. vid platsspecifik underrättelseinhämtning, upptäcks farliga föremål eller ämnen är det möjligt att gå till väga på det sätt som föreskrivs i 2 kap. 14 och 15 § i polislagen. Till denna del finns det anledning att också vara uppmärksam på att om det i ett utrymme där platsspecifik underrättelseinhämtning utförs påträffas farliga föremål eller ämnen och dessa eventuellt har bytts ut även mot ofarliga, är det högst sannolikt att tröskeln för ”anledning att misstänka” ett brott som ska förhindras eller avslöjas eller något annat i strafflagen avsett brott har överskridits. Då gäller det att gå över från att använda metoder för underrättelseinhämtning till att utöva brottsrelaterade befogenheter, vilket inte längre är militär underrättelseinhämtning. I den situationen bör underrättelseinhämtningen avslutas.

När man i samband med platsspecifik underrättelseinhämtning t.ex. fotograferar dokument som påträffats i ett utrymme som är föremål för den platsspecifika underrättelseinhämtningen, kopieras dokumentet på samma gång. Under eller strax efter den platsspecifika underrättelseinhämtningen står det inte nödvändigtvis klart vilken betydelse dokumenten har, och klarläggandet av dokumentens informationsinnehåll kan förutsätta t.ex. att dokumenten översätts.

2.4.4.8 Informationsinhämtning i datanät och datasystem

*Underrättelseinhämtning som avser datatrafik*

Som ovan konstateras angående teleavlyssning och metoder för inhämtning av telekommunikationsuppgifter möjliggör de gällande befogenheterna till inhämtning av telekommunikationsuppgifter inte att Försvarsmakten i underrättelsesyfte inhämtar information om kommunikation som sker i datakommunikationsnät och går via Finland. I och med den tekniska ut-

vecklingen sker numera också t.ex. de väpnade styrkornas meddelandetrafik i huvudsak via datakommunikationsnät.

Det är tekniskt möjligt att i den elektroniska kommunikationsmiljön upptäcka, identifiera och organisera militära aktiviteter och verksamhet som utgör ett hot mot den nationella säkerheten. För att förmåga att upptäcka och identifiera ska kunna skapas förutsätts det emellertid en lösning som till sina grundläggande egenskaper avviker från de nuvarande metoderna för inhämtning av telekommunikationsuppgifter och där informationsinhämtningen sker med hjälp av ett system som filtrerar meddelande- och datatrafikflödet. Nättopologiskt sett innebär detta att informationsinhämtningen, tvärtemot vad som är fallet med de metoder för inhämtning av telekommunikationsuppgifter som den gällande lagstiftningen möjliggör, genomförs mitt i det internationella kommunikationsnätet. Avsikten med att filter som används vid informationsinhämtning placeras mitt i kommunikationsnätet är att säkerställa att det genom systemet med så stor sannolikhet som möjligt flödar sådan meddelande- eller datatrafik som kan förmodas hänföra sig till verksamhet som är föremål för militär underrättelseinhämtning. Vid sållningen separeras sådan kommunikation som är relevant med tanke på hot från den övriga datatrafiken med hjälp av vissa i förväg fastställda kriterier eller sållningsparametrar. Som sållningsparametrar kan fastställas t.ex. särskilda kommunikationsmetoder, produktidentifiering för utrustning som används för att transportera meddelanden, IP-adressrymder eller information som anger tidpunkt och plats för kommunikationen, om de enligt vad man vet hänför sig till den verksamhet som informationsinhämtningen riktas mot.

Ett tillvägagångssätt som grundar sig på sållning torde till vissa delar kunna jämställas med profilering som säkerhetsmyndigheterna använder inom annan verksamhet och med vars hjälp avvikelser som är relevanta från säkerhetssynpunkt letas fram i en större målgrupp. Till sin karaktär kan sållning av meddelandetrafik jämställas med t.ex. gräns- och tullövervakning som bygger på profilering och riskbedömning. Inom gräns- och tullövervakningen kan en del av dem som överskrider landets gränser bli föremål för närmare undersökning därför att de motsvarar vissa i förväg angivna sållningsparametrar som gäller t.ex. resesättet.

Sållning av meddelandetrafiken kan ändå baseras förutom på allmän kunskap om människors beteende eller verksamhetssätt också på konkret information som beskriver ett hot som är föremål för informationsinhämtning. Som exempel på sådan information kan nämnas information om att det i kommunikation som rör ett hot som är föremål för informationsinhämtning används en sådan programkod eller kryptering som endast en specifik militär organisation använder.

Den internationella jämförelsen visar att de flesta jämförda länderna har valt att använda eller planerar att ta i bruk sådana metoder för informationsinhämtning som grundar sig på sållning av meddelande- och datatrafiken. Trots skillnaderna mellan dessa metoder kan metoderna gemensamt benämnas underrättelseinhämtning som avser datatrafik. Avsikten med den underrättelseinhämtning som avser datatrafik som de jämförda länderna använder eller planerar att ta i bruk är att upptäcka hot mot den nationella säkerheten, identifiera personerna bakom hoten samt identifiera teleadresser och teleterminalutrustning som används i den verksamhet som utgör ett hot för att möjliggöra teleavlyssning och teleövervakning, och att inhämta mer detaljerad information om hoten.

I de jämförda länderna används underrättelseinhämtning som avser datatrafik som en metod för underrättelseinhämtning, inte som ett medel att förhindra, avslöja eller utreda brott. Syftet med underrättelseinhämtningen är inte att med tanke på en framtida straffrättslig process inhämta information om en person som är känd i förväg och som på goda grunder kan antas

göra eller misstänkas ha gjort sig skyldig till brott av en viss allvarlighetsgrad, utan syftet är upptäcka och identifiera hot mot de viktigaste nationella säkerhetsintressena och att dela med sig av analyserad information om hoten till parter som behöver den. Underrättelseinhämtning som avser datatrafik skiljer sig från polisens hävdvunna metoder för inhämtning av telekommunikationsuppgifter och annan information och också från de flesta metoder som underrättelsetjänsterna använder, just därför att den till följd av sina tekniska särdrag möjliggör effektivare underrättelseinhämtning än förr om t.ex. militära aktiviteter.

De sållningsparametrar som används vid underrättelseinhämtning som avser datatrafik och som kan benämnas sökbegrepp kan sålla innehållet eller annan information i meddelande- och datatrafik som flödar igenom underrättelsesystemet. Med annan information avses t.ex. information som behövs för att styra enskilda meddelanden i datatrafikflödet från avsändaren till mottagaren samt information om tidpunkt och plats för kommunikationen.

Hur effektiv underrättelseinhämtning som avser datatrafik är och vilka konsekvenser den har för de grundläggande fri- och rättigheterna är beroende av om man som sökbegrepp använder information som beskriver meddelandets innehåll eller bara annan information som hänför sig till kommunikationen. Effektiviteten kan vara större om man som sökbegrepp kan använda information som beskriver meddelandets innehåll. Då behöver underrättelsemyndigheten inte ha förhandskännedom om t.ex. vilken adressrymd parterna kommunicerar i, utan det går att bland alla meddelanden i datatrafikflödet leta fram exempelvis sällsynta namn eller koduttryck som enligt vad man vet eller kan anta används t.ex. i samband med spionage som en främmande makt bedriver och som är föremål för utredning. Att använda sökbegrepp som beskriver meddelandets innehåll behövs därmed framför allt när det inte är känt vilka kommunikationskanaler som används i den verksamhet som är föremål för informationsinhämtning, eller när kännedomen om dem är på ett mycket allmänt plan.

Användningen av innehållsrelaterade sökbegrepp utgör visserligen ett större ingripande i förtrolig kommunikation än användningen av andra sökbegrepp, eftersom den förutsätter att all genomflödande kommunikation, även kommunikation som alla som inte har något med hotet att göra ägnar sig åt, öppnas och att sökbegreppen jämförs mot meddelandenas innehåll. Innehållsrelaterade sökbegrepp avgränsar inte heller nödvändigtvis mängden information som inhämtas, t.ex. på grund av de betydelseinnehåll som personer ger vissa ord.

I alla jämförda länder där det finns eller bereds lagstiftning om underrättelseinhämtning som avser datatrafik är det eller planeras det bli tillåtet att använda sökbegrepp som beskriver innehållet i kommunikationen. Användningen av innehållsrelaterade sökbegrepp är emellertid avgränsad antingen i lag eller i lagmotiven på ett sådant sätt att det inte är tillåtet att som sökbegrepp använda vanliga uttryck som ingår i allmänspråket. Sökbegrepp som kan tillåtas är därmed närmast sådana sällsynta personnamn och uttryck som inte är allmänt kända eller inte är i allmänt bruk, och som därmed inte kan antas förekomma när utomstående personer kommunicerar med varandra.

De innehållsrelaterade sökbegreppens användbarhet och effektivitet begränsas av den krypteringstekniska utvecklingen och krypteringsteknikernas spridning. Annan information som anknyter till kommunikation kan inte krypteras på samma sätt som innehållet i meddelanden, eftersom den behövs för att styra meddelandena från avsändaren till mottagaren i kommunikationsnätet. Den betydelse som informationen om styrning och förmedling av kommunikationen har som sökbegrepp vid underrättelseinhämtning som avser datatrafik är därför stor. I det betänkande som arbetsgruppen för en informationsanskaffningslag gav bedöms det (s. 76) att man genom underrättelseinhämtning som avser datatrafik trots kryptering kan få information

som är av betydelse med tanke på den nationella säkerheten, t.ex. utgående från identifieringsuppgifter.

Underrättelseinhämtning som avser datatrafik kan användas för att upptäcka, identifiera och utreda dels yttre hot mot det land som bedriver underrättelseinhämtning, dels rent interna hot. I de jämförda staterna används underrättelseinhämtning som avser datatrafik för att upptäcka, identifiera och utreda enbart yttre hot, alltså som en metod för underrättelseinhämtning som avser utländska förhållanden. Som en följd av detta har underrättelseinhämtning som avser datatrafik organiserats på ett sådant sätt i de jämförda staterna att den riktar sig mot meddelande- och datatrafik som överskrider den underrättelseinhämtande statens gräns.

Av de jämförda staternas lagstiftningar och lagmotiveringar kan man sluta sig till att underrättelseinhämtning som avser datatrafik i dessa stater har organiserats eller avses bli organiserad i form av verksamhet som omfattar flera etapper. Trots skiljaktigheterna mellan de olika ländernas lagstiftningar kan verksamheten generaliserat karaktäriseras som så att bland de gränsöverskridande datakommunikationsförbindelserna väljs först de delar ut genom vilka man kan anta att det flödar sådan kommunikation eller annan datatrafik som anknyter till verksamhet som är föremål för underrättelseinhämtning. Kommunikationen och den övriga datatrafiken i de utvalda datakommunikationsförbindelserna antingen styrs så att den går genom ett datasystem som används för underrättelseinhämtning, eller så skapar man av den en kopia som sparas. I det förstnämnda fallet jämför datasystemet den genomflödande kommunikationen och datatrafiken i realtid mot de i förväg uppställda sökbegreppen. Den kommunikation och övriga datatrafik som motsvarar sökbegreppen styrs till en analysdatabas för fortsatt behandling. Kommunikation och datatrafik av annat slag går igenom underrättelsesystemet och kan längre fram inte återställas för att granskas. I det sistnämnda fallet används sökbegreppen inte i realtid, utan hela den kopierade trafiken styrs till en analysdatabas där sökningar senare kan göras.

I ett tidigare avsnitt i denna proposition beskrivs människorättsdomstolens och EU-domstolens rättspraxis till den del den är relevant för organiseringen av underrättelseinhämtning som avser datatrafik. Av beskrivningen framgår att människorättsdomstolen har ansett att sådan underrättelseinhämtning som avser datatrafik och som organiseras under vissa jämförelsevis stränga specialvillkor är förenlig med artikel 8 i människorättskonventionen.

När man bedömer huruvida underrättelseinhämtning som avser datatrafik kan tillåtas med tanke på människorättskonventionen och ur EU-rättsligt perspektiv är särskilt den omständigheten att den nationella lagstiftningen är förenlig med proportionalitetsprincipen av betydelse, enligt internationell domstolspraxis. Människorättsdomstolens syn på de minimikrav som proportionalitetsprincipen medför uttrycks i ett test som domstolen inlemmat i sina avgöranden i rättsfallen Huvig mot Frankrike 24.4.1990 och Kruslin mot Frankrike 24.4.1990. I senare avgöranden har människorättsdomstolen upprepade gånger tillämpat testet, och i viss mån också vidareutvecklat det. Också i det avgörande som EU-domstolen träffade i rättsfallet Digital Rights Ireland var det till stor del fråga om att tillämpa det ovannämnda testet, som går under namnet Huvig/Kruslin-testet. Enligt testet ska nationell lagstiftning som berättigar till att ingripa i kommunikationshemligheten innehålla följande: 1) en definition av vilka personers kommunikationshemlighet det ingrips i, 2) en definition av vilka gärningar eller hot som ger anledning att ingripa i kommunikationshemligheten, 3) bestämmelser om hur det ska beslutas om ingripandet, 4) bestämmelser om hur informationen ska behandlas, användas och bevaras, 5) bestämmelser om varaktigheten för ingripandet i kommunikationshemligheten och om bevaringstiderna för den information som insamlats genom åtgärderna, 6) försiktighetsåtgärder

som ska vidtas när information lämnas ut till andra och 7) förfaranden som ska iakttas när information gallras ut och utplånas.

Som ovan konstateras tillåter de internationella människorättskonventionerna som är bindande för Finland underrättelseinhämtning som avser både intern och gränsöverskridande datatrafik, förutsatt att vissa specialvillkor uppfylls. Eftersom de allvarligaste hoten mot Finlands nationella säkerhet är yttre hot i första hand, hänför sig Finlands behov till underrättelseinhämtning i fråga om gränsöverskridande datatrafik. De hot som underrättelseinhämtning som avser datatrafik får inriktas på bör för sin del definieras på lagnivå så entydigt och snävt som möjligt. Hoten bör till sin natur vara militära eller tillräckligt allvarliga och riktas mot säkerhetsintressen som är centrala med tanke på den nationella säkerheten. Det kan anses vara klart att underrättelseinhämtning som avser datatrafik inte kan vara en metod som används för undersökning av nätbrottslighet eller annan massbrottslighet som är att betrakta som ordinär. Utgångspunkten bör vara att det inte ska tillåtas att underrättelseinhämtning som avser datatrafik används som brottsutredningsmetod.

Underrättelseinhämtning som avser sådan datatrafik som överskrider Finlands gräns bör genomföras på ett sådant sätt att man bland datatrafiken så effektivt som möjligt kan sålla fram datatrafik som är relevant med tanke på allvarliga hot som ligger till grund för underrättelseverksamheten och förhindra att trafik som inte hänför sig till uppdragen blir föremål för analys. Vid sållningen bör man därför använda tillräckligt exakta sökbegrepp som bestämts i förväg eller sådana verbala beskrivningar av verksamhet som äventyrar den nationella säkerheten vilka så konkret som möjligt karaktäriserar föremålet för informationsinhämtning. Föremålen för beskrivningen kan vara sådana kommunikationsmodeller och verksamhetsmodeller av andra slag som enligt vad man vet eller kan anta anknyter till verksamhet som äventyrar den nationella säkerheten. Godkännandet av sökbegrepp och verbala beskrivningar bör skötas av en tillståndsmyndighet som är fristående från underrättelsemyndigheten, och användningen av dem vid underrättelseinhämtning bör dokumenteras ingående med tanke på övervakningen i efterhand. En domstol kan fungera som tillståndsmyndighet. Inrättandet av ett nytt oavhängigt organ för laglighetsövervakning som ska sköta övervakningen i efterhand kan övervägas.

De sökbegrepp som tillåts vid underrättelseinhämtning som avser datatrafik kan begränsas så att endast sådan information som inte gäller meddelandets innehåll kommer i fråga. Som exempel på sådana sökbegrepp kan nämnas identifieringsuppgifter som beskriver nätverksutrustning och nätadresser samt information som beskriver tidpunkt och plats för kommunikationen. När det gäller underrättelseinhämtning som avser datatrafik föreslås det att man i Finland intar en sådan ståndpunkt till användningen av innehållsrelaterade sökbegrepp som skiljer sig från de ovan jämförda ländernas lagstiftningar och är strängare. Ett undantag från detta utgör situationer där underrättelseinhämtning som avser datatrafik riktar sig enbart mot en statlig aktörs datatrafik.

När syftet med underrättelseinhämtning som avser datatrafik är att upptäcka nätspionage som genomförs via sabotageprogram bör emellertid undantagsvis också sökbegrepp som beskriver meddelandets innehåll kunna användas. Signaturer som identifierar sabotageprogram kommer då i fråga som sökbegrepp som beskriver innehållet.

Sållningen av signal- och datatrafik med hjälp av sökbegrepp sköts maskinellt i cacheminnet i systemet för underrättelseinhämtning som avser datatrafik. Meddelanden som separerats från den övriga datatrafiken med hjälp av sökbegrepp och som i princip kan antas vara relevanta när det gäller att utreda ett hot som är föremål för informationsinhämtning föreslås kunna tas upp till manuell behandling, och då får också meddelandenas innehåll klarläggas. Meddelan-

den som på basis av att innehållet klarlagts konstateras hänföra sig till det hot som underrättelseinhämtningen är inriktad på får sparas. Överskottsinformation som inte har någon anknytning till den militära underrättelseinhämtningens uppdrag ska däremot utplånas omedelbart efter att den konstaterats vara av detta slag.

Eftersom underrättelseinhämtning som avser datatrafik har syftet att inhämta information om yttre hot i datatrafik som överskrider Finlands gräns ska datatrafik mellan parter som befinner sig i Finland utplånas, om den av tekniska skäl fångas upp vid underrättelseinhämtning som avser datatrafik.

Mer generellt kan det sägas om behandlingen av information som erhållits genom underrättelseinhämtning som avser datatrafik att människorättsdomstolens rättspraxis förutsätter att det på lagnivå föreskrivs tillräckligt exakt om hur informationen ska granskas och kan utnyttjas, om bevaringstiderna för informationen samt om utlämnande och utplåning av den. När det gäller t.ex. utlämnande av information till en utländsk myndighet bör utgångspunkten vara att utlämnandet av information främjar den nationella säkerheten och inte äventyrar Finlands intressen, bland dem också samhällsekonomiska intressen.

När det föreskrivs på det föreslagna sättet om underrättelseinhämtning som avser datatrafik blir följden inte sådan omfattande, ospecificerad, långvarig och obegränsad lagring av identifieringsuppgifter som i de internationella domstolarnas rättspraxis har ansetts strida mot proportionalitetsprincipen.

För att förhandsvarningar ska kunna ges effektivt och för att kännedomen om situationen i verksamhetsmiljön ska vara god bör Försvarsmakten ha behövliga befogenheter att utföra gränsöverskridande underrättelseinhämtning som avser datatrafik. Varje part som äger eller innehar ett kommunikationsnät som överskrider Finlands gräns eller en del av ett sådant bör bistå myndigheten när underrättelseinhämtning som avser datatrafik utförs. En bistående part kan benämnas dataöverförare. Biståndsskyldigheten är jämförbar med den skyldighet för teleföretag att bistå vid teleavlyssning och teleövervakning som följer gällande lagstiftning. Det bör föreskrivas separat om teleföretagens biståndsskyldighet.

*Inhämtande av information om hot från internet*

Parter som hotar landets försvar eller den nationella säkerheten kan använda elektroniska kommunikationsnät inte bara för kommunikation som hänför sig till hot utan också för att verkställa hot. På det sätt som konstaterats i ett tidigare avsnitt i denna proposition kan cybergärningar som utförs via kommunikationsnät, t.ex. cyberspionage, massiva cyberattacker, cyberoperationer som inbegriper påtryckningar och cybersabotage som riktas mot vitala statsfunktioner, i värsta fall äventyra statens livsduglighet eller statens centrala säkerhetsintressen. Vid sidan av staten kan cybergärningar också riktas mot privata företag eller sammanslutningar, varvid gärningarna äventyrar t.ex. deras produktutvecklingsinformation som är avsedd att vara hemlig.

En förutsättning för att cyberhot ska kunna förhindras eller för att åtminstone de skadliga följderna av dem ska kunna begränsas är att hoten upptäcks i ett tillräckligt tidigt skede. Försvarsmaktens metoder för informationsinhämtning lämpar sig inte för att upptäcka gärningar som begås i cyberomgivningen, eftersom Försvarsmakten saknar befogenheter att inhämta information om dessa hot. Också enligt den reglering som för närvarande gäller i Finland är det en förutsättning för användningen av metoder för inhämtning av telekommunikationsuppgifter att föremålet för metodanvändningen, i fråga om metoder för inhämtning av telekommunikat-

ionsuppgifter teleadressen eller teleterminalutrustningen och i fråga om t.ex. metoder med karaktären av observation personen, är känd när informationsinhämtningen påbörjas.

I den regleringsmiljö som råder i Finland beror den omständigheten att metoderna för inhämtning av telekommunikationsuppgifter inte är särskilt lämpliga för upptäckande av cyberhot också på cyberhotens särdrag. Cybergärningar som riktas mot Finland och Finlands nationella säkerhet verkställs i allmänhet utanför landets gränser, och genomförandet förutsätter inte någon som helst fysisk närvaro på finskt territorium. Därför kan de finska myndigheterna inte ens i princip komma underfund med gärningarna före det ögonblick då den anfallsvektor som används i samband med gärningen, i regel ett tekniskt sabotageprogram, överskrider Finlands gräns i ett kommunikationsnät. Intervallet mellan den tidpunkten och uppkomsten av skadliga följder som gärningen orsakar kan vara mycket kort. Gärningar som i sin helhet genomförs i elektroniska kommunikationsnät kan dessutom genomföras med hjälp av närapå vilken teleadress eller teleterminalutrustning som helst. Den som begår en cybergärning behöver inte använda, och använder heller i regel inte, en teleadress eller teleterminalutrustning som befinner sig i eller annars kan associeras till det land som ligger bakom gärningen eller där förövaren befinner sig i övrigt. Cyberomgivningen erbjuder ypperliga möjligheter att vilseleda föremålet för gärningen och sopa igen spåren efter förövaren. Sammanfattningsvis är det utmärkande för gärningar som begås i cyberomgivningen och hotar den nationella säkerheten att kostnaderna för att begå dem är låga, samma vektorer kan användas upprepade gånger och riktas mot flera objekt, det är svårt och kostsamt att skydda sig mot gärningarna och risken för att åka fast är liten.

Möjligheterna att upptäcka och förhindra cybergärningar som äventyrar den nationella säkerheten baserar sig i nuläget huvudsakligen på befogenheterna i 272 § i informationssamhällsbalken.

Skadliga program och kommandon identifieras i den första etappen genom automatisk innehållsanalys som grundar sig på specifikationer som gjorts i förväg. Om det är uppenbart att ett meddelande som sticker ut vid den automatiska analysen innehåller ett sabotageprogram och informationssäkerheten inte går att säkerställa på automatisk väg tillåter bestämmelserna i 272 § i informationssamhällsbalken att ett företag, en sammanslutning eller en myndighet behandlar meddelandets innehåll manuellt.

Vid utövandet av den rätt att vidta åtgärder som följer av 272 § i informationssamhällsbalken, det må sedan ske inom ett företag, en sammanslutning eller en myndighet som sörjer för sin informationssäkerhet eller inom ramen för systemet Havaro, är det från teknisk synpunkt till stor del fråga om liknande sållning av datatrafik utifrån sökbegrepp och vidarebehandling av meddelanden som sticker ut vid sållningen som i underrättelseinhämtning som avser datatrafik, en metod som föreslås i denna proposition. I verksamhet enligt 272 § i informationssamhällsbalken används som sökbegrepp bl.a. signaturer som beskriver sabotageprogrammens innehåll, identifieringsuppgifter för teleadresser som används för att sprida sabotageprogram samt identifikatorer som beskriver sådana sätt att trafikera som är typiska för sabotageprogram. Förmågan att upptäcka sabotageprogramtrafik som hotar den nationella säkerheten är beroende av kvaliteten på de signaturer och andra identifikationer för sabotageprogram som används som sökbegrepp vid sållningen.

De signaturer för sabotageprogram som företag, sammanslutningar och myndigheter använder i sin verksamhet är i regel sådana som är i kommersiellt bruk eller annars allmänt tillgängliga. De identifikatorer som matas in i Havaro baserar sig främst på sådan information som Cybersäkerhetscentret vid Kommunikationsverket har fått via sina nationella och internationella

kontakter. Bland Cybersäkerhetscentrets viktigaste internationella samarbetsparter finns de s.k. GovCERT-grupperna i olika länders statsförvaltningar.

Till de sabotageprogram som det är svårast att upptäcka och som samtidigt skadar den nationella säkerheten mest hör statliga spionprogram och andra statliga sabotageprogram. Möjligheterna att upptäcka sådana sabotageprogram inom ramen för åtgärder för informationssäkerheten som företag, sammanslutningar och myndigheter själva vidtar eller via systemet Havaro är begränsade. Orsaken är framför allt att signaturer och motsvarande som är nödvändiga för att upptäcka spionage och annan fientlig verksamhet från statligt håll inte används av de parter med rätt att vidta nödvändiga åtgärder som avses i 272 § i informationssamhällsbalken, och inte heller kan de läggas in i Havaro. De signaturer och motsvarande som behövs för att upptäcka verksamhet är information som omfattas av hög skyddsnivå och som i typiska fall utbyts i det internationella samarbete som säkerhets- och underrättelsetjänsterna bedriver. Samarbetet grundar sig på parternas förtroende för varandra. Ett villkor för utlämnande av information inom ramen för samarbetet är nästan utan undantag att det är förbjudet att låta informationen gå vidare till utomstående. Eftersom Cybersäkerhetscentret vid Kommunikationsverket, den aktör som förvaltar Havaro, varken är eller kan vara part i samarbetet säkerhets- och underrättelsetjänsterna emellan utan är utomstående i förhållande till samarbetet är det inte möjligt att lämna ut till Havaro sådana identifikationer som skulle ha den största betydelsen med tanke på skyddet av den nationella säkerheten.

Syftet med de åtgärder för informationssäkerheten som möjliggörs genom 272 § i informationssamhällsbalken, Havaro inräknad, är att informationssäkerheten ska genomföras genom att enskilda organisationer skyddas mot kränkningar som riktas mot dem. Syftet med åtgärderna för informationssäkerheten är inte att täcka informationsbehov som anknyter till avvärjandet av verksamhet som äventyrar den nationella säkerheten.

Med tanke på åtgärderna för informationssäkerheten är information som är väsentlig för att den nationella säkerheten ska upprätthållas, t.ex. orsakerna och bakgrundsmotiven till de allvarligaste kränkningarna av informationssäkerheten, förövarnas identitet och de förhållanden under vilka kränkningarna utförs, inte central.

Ovan konstateras det att verksamhet som avses i 272 § i informationssamhällsbalken tekniskt sett har stora likheter med den verksamhet som beskrivs i den internationella jämförelsen i denna proposition och som sammanfattningsvis kan benämnas underrättelseinhämtning som avser datatrafik. Av funktionernas tekniska likheter följer att ett system för underrättelseinhämtning som avser datatrafik och baserar sig på filtrering av datatrafik utgående från sökbegrepp kan användas också för identifiering av sabotageprogram.

I de jämförda staterna intar underrättelseinhämtning som avser datatrafik en viktig ställning, inte bara inom traditionell underrättelseinhämtning som riktas mot verksamhet som hotar den nationella säkerheten utan också som en metod att upptäcka cyberhot och skydda sig mot dem (t.ex. betänkandet ”En anpassad försvarsunderrättelseverksamhet”). Departementsserien 2005:30. Regeringskansliet/Försvarsdepartementet, s. 96–99). Underrättelseinhämtning som avser datatrafik möjliggör framför allt upptäckter av sådana cyberhot som äventyrar samhällets centrala säkerhetsintressen på de allra allvarligaste sätten.

*Underrättelseinhämtning som avser utländska datasystem*

Arbetsgruppen för en informationsanskaffningslag konstaterade i sitt betänkande att det bör föreskrivas för säkerhetsmyndigheterna om befogenheter till underrättelseinhämtning som av-

ser utländska datasystem. Med underrättelseinhämtning som avser utländska datasystem avses att information som behandlas i ett utländskt datasystem inhämtas med datatekniska metoder.

Underrättelseinhämtning som avser utländska datasystem kan företas på så sätt att metoder för teknisk observation av utrustning och, till vissa delar, teknisk avlyssning utnyttjas. Eftersom underrättelseinhämtning som avser utländska datasystem är långvarig verksamhet och förutsätter noggrann identifiering av eventuella utrikespolitiska kontaktytor med tillhörande överväganden, kan det inte anses att teknisk observation av utrustning och teknisk avlyssning är ändamålsenliga metoder för informationsinhämtning till denna del. Ser man till den helhet som underrättelseinhämtning som avser utländska datasystem utgör kan det inte anses vara ändamålsenligt att användningen av den skulle förutsätta två separata tillståndsprövningar.

Finska myndigheter har inte befogenheter att företa informationsinhämtning utanför Finlands gränser, inte ens om informationsinhämtningen sker utgående från finskt territorium och riktar sig mot ett datasystem i utlandet. Dessutom är det ändamålsenligt att vid underrättelseinhämtning som avser utländska datasystem förbigå skyddet för datasystemet med datatekniska metoder, något som i avsaknad av en explicit bestämmelse om detta inte är möjligt för finska myndigheter.

Inom underrättelseinhämtning som avser utländska datasystem gäller det på grund av verksamhetens särdrag att ta hänsyn också till utrikes- och säkerhetspolitiska omständigheter.

2.4.5 Beslutsfattande

Rätten att fatta beslut om användning av vissa hemliga metoder för inhämtande av information som Försvarsmakten använder är så som ovan nämns fördelad mellan domstolen, den biträdande avdelningschef vid Huvudstaben som svarar för kontraspionaget och en militärjurist.

Sammanfattningsvis kan det konstateras angående de hemliga metoder för inhämtande av information som anges i lagen om militär disciplin och brottsbekämpning inom försvarsmakten och 5 kap. i polislagen att av de i 5 kap. i polislagen nämnda befogenheterna förutsätter teleavlyssning, inhämtande av information i stället för teleavlyssning och inhämtande av basstationsuppgifter ett domstolstillstånd. Oftast är domstolen också behörig att besluta om teleövervakning. I sådana brådskande situationer där polisen tillfälligtvis kan besluta själv om teleövervakning ska ärendet föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas. Polisen kan emellertid besluta om teleövervakning för att avvärja fara som hotar liv eller hälsa, och med samtycke av den som innehar en teleadress eller teleterminalutrustning får polisen besluta om teleövervakning vid misstanke om brott som har en direkt anknytning till teleadressen eller teleterminalutrustningen.

Ett yrkande 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 ha 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.

Enligt 5 kap. 58 § i polislagen ska den som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning och teleövervakning underrättas om detta utan dröjsmål 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. På yrkande av en anhållningsberättigad polisman får domstolen emellertid 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 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 till teleavlyssning och teleövervakning i en majoritet av fallen. Ett fåtal avslagsbeslut uppskattas förekomma varje år. År 2015 avslog domstolarna elva yrkanden på teletvångsmedel som polisen hade framställt. Samtliga avslag gällde ansökningar som grundade sig på tvångsmedelslagen.

Lagen om militär underrättelseverksamhet grundar sig till väsentliga delar på regleringen i 5 kap. i polislagen. Den ståndpunkt som betonar att ett ingripande i de grundläggande fri- och rättigheterna och de mänskliga rättigheterna är betydande talar för att domstolens beslutsbefogenheter bör förbli i hög grad oförändrade i fråga om de hemliga metoder för inhämtande av information som står till förfogande i dagens läge. De metodspecifika ingripanden i de grundläggande fri- och rättigheterna och de mänskliga rättigheterna som anknyter till befogenheten att fatta beslut bedömdes i samband med förundersöknings- och tvångsmedelskommissionens arbete (justitieministeriets kommittébetänkande 2009:2). Därför är det befogat att så långt som möjligt följa regleringen i 5 kap. i polislagen också i fråga om de grundläggande lösningar i lagen om militär underrättelseverksamhet som gäller fattande av beslut om metoderna för underrättelseinhämtning.

Reglering behövs inte bara när det gäller metoderna för underrättelseinhämtning utan också i fråga om fattandet av beslut om underrättelseinhämtning som avser utländska förhållanden. Domstolen är i princip inte behörig att besluta om utövande av befogenheter annanstans än i Finland. På grund av de utrikespolitiskt sensitiva elementen i samband med underrättelseinhämtning som avser utländska förhållanden är det inte heller ändamålsenligt att operativt beslutsfattande anförtros nya aktörer i det rättsliga systemet.

I vissa länder som ingår i den internationella jämförelsen och i en del andra länder beslutar chefen för underrättelsetjänsten om underrättelseinhämtning som avser utländska förhållanden. Det är motiverat att föreskriva på motsvarande sätt om beslutsfattandet i fråga om militär underrättelseinhämtning som avser utländska förhållanden. Med stöd av 5 kap. i polislagen beslutar chefen för skyddspolisen för närvarande om användning av de allra mest drastiska metoderna, dvs. täckoperationer och bevisprovokation genom köp. Vid beslutsprövningen för deras del behöver det tas ställning till omständigheter av motsvarande allvarlighetsgrad som vid beslutsfattande om underrättelseinhämtning som avser utländska förhållanden. Det är ändamålsenligt att beslutsfattandet för den militära underrättelseinhämtningens vidkommande är på samma nivå, varvid besluten kan fattas av Huvudstabens underrättelsechef.

Eftersom omständigheter som tangerar flera förvaltningsområden är förknippade med underrättelseinhämtning som avser utländska förhållanden bör det säkerställas att tvärsektoriella synpunkter beaktas vid beslutsfattandet.

Av de ovannämnda skälen är det befogat att också regleringen om underrättelse om användning av metoder för underrättelseinhämtning motsvarar regleringen i 5 kap. i polislagen, förutsatt att särdragen hos den militära underrättelseinhämtningen beaktas.

2.4.6 Bestämmelser som är gemensamma för alla hemliga metoder för inhämtande av information

2.4.6.1 Skyddande av informationsinhämtning

Försvarsmakten kan inte skydda informationsinhämtning med stöd av bestämmelserna om befogenheter vid brottsbekämpning. I polislagen, som fungerar som jämförelseobjekt, föreskrivs det i 5 kap. 46 § om skyddande av hemligt inhämtande av information. Bestämmelserna i 1 mom. i den paragrafen gäller polisens möjlighet att dröja med att ingripa i brott under tiden för hemligt inhämtande av information. En förutsättning 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 2 mom. får polisen använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt framställa 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 den nuvarande regleringen kan skydd tillämpas i samband med alla hemliga metoder för inhämtande av information (även vid förtäckt inhämtande av information), eftersom behovet kan framgå t.ex. vid teleövervakning som polisen utför med sin egen utrustning. Med stöd av momentet kan varken en informationskälla eller någon annan utomstående emellertid ges en täckidentitet, utan syftet är att skydda verksamheten.

Görandet av registeranteckningar och andra anteckningar med oriktigt innehåll behandlas i riksdagens biträdande justitieombudsmans avgörande 571/2/08. Frågan hänför sig till de spänningar som förekommer i och med att polisen har undersökningstvång och det krävs att registreringar är lagenliga, men detta inte är förenligt med sekretessintressena i samband med bevisprovokation genom köp och täckoperationer. Lagen ger inte ett tydligt svar på t.ex. frågan om huruvida och i vilken mån det är möjligt att utarbeta förundersökningsprotokoll eller undersökningsanmälningar med oriktigt innehåll för att förhindra att en hemlig metod för inhämtande av information avslöjas.

I många fall är det fråga om intresseavvägning och helhetsprövning. Utgångspunkten är att skyddsmetoder inte bör tillgripas lättvindigt eftersom skyddet är förknippat med problem och av rättsskyddsskäl. Utgångspunkten är att upprättandet av ett falskt myndighetsdokument föranleder också en falsk registeranteckning i myndighetsregister som åtnjuter offentligt förtroende. Därför bör ett skydd vara nödvändigt.

Falska anteckningar får dock inte kvarstå i registren, utan i 3 mom. föreskrivs det att registeranteckningarna ska rättas.

Det finns ett accentuerat behov av att föreskriva om nämnda slag av skyddande av informationsinhämtning också för att skydda den militära underrättelseinhämtningen. Utgångspunkten är att hela den militära underrättelseverksamheten bör kunna skyddas. Med underrättelseverksamheten sammanhänger många slag av sensitiva element och föremålet för den kan vara en

annan stats förvaltning, en enskild person eller en grupp av personer som är av stort intresse, någon industrigren eller ett enskilt företag. I praktiken vill man genom underrättelseinhämtning inhämta information utan att föremålet för verksamheten är medvetet om saken och oberoende av detta objekts vilja. För att risken för att bli avslöjad ska minimeras bör användningen av skydd möjliggöras redan på ett tidigt stadium. För att t.ex. landets egna tjänstemän som använder en metod för underrättelseinhämtning ska skyddas genom infiltrering av en främmande stats kontraspionageorganisation förutsätts skyddsåtgärder som är avsevärt intensivare och påbörjas i ett mycket tidigt skede, t.ex. genom en täckoperation. Inom den militära underrättelseverksamheten förekommer inte heller motsvarande rättsskyddsproblem vad gäller skyddande som när brottsrelaterade befogenheter utövas, eftersom det primära syftet för den militära underrättelseinhämtningen är att inhämta information om verksamhet som hotar landets försvar eller allvarligt hotar den nationella säkerheten.

2.4.6.2 Förbud mot avlyssning och observation

Bestämmelser om de ovan refererade förbuden mot avlyssning och observation har utfärdats med tanke på straffprocessen och straffprocessuella tvångsmedel. Även om förbuden mot avlyssning och observation intar en viktig ställning också inom den civila underrättelseinhämtningen framstår deras status som en annan än i straffprocessen. Inom den militära underrättelseinhämtningen bör de nämnda förbuden nästan uteslutande bedömas vara förbud som inte anknyter till straffprocessen och som saknar en direkt koppling till rättsskyddet för den brottsmisstänkte. Metoderna för underrättelseinhämtning ingriper emellertid i de grundläggande och mänskliga rättigheterna lika väl som de hemliga metoderna för inhämtande av information, trots att det egentliga syftet med metoderna för underrättelseinhämtning inte är straffprocessuellt. Vad beträffar användningen av de metoder för underrättelseinhämtning som är i bruk inom den militära underrättelseinhämtningen bör man föreskriva om förbud mot avlyssning och observation lika väl som beträffande användningen av andra hemliga metoder för inhämtande av information.

Med avvikelse från det som i polislagen och tvångsmedelslagen föreskrivs om förhindrande, avslöjande och utredande av brott är det meningen att metoder för underrättelseinhämtning inte ska riktas mot en brottsmisstänkt eller en förmodad framtida gärningsman. Den militära underrättelseinhämtningen handlar om att inhämta information om militär aktivitet eller om verksamhet som allvarligt hotar den nationella säkerheten.

På grund av den militära underrättelseinhämtningens särdrag bör det föreskrivas att teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning och optisk observation inte får riktas mot sådan kommunikation som en part 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 det om en skyldighet för ett rättegångsombud, ett rättegångsbiträde eller en tolk att 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. I paragrafen föreskrivs dessutom om en skyldighet för en advokat, ett rättegångsbiträde som avses i lagen om rättegångsbiträden med tillstånd eller ett offentligt rättsbiträde 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. I 17 kap. 14 § i rättegångsbalken föreskrivs det om en skyldighet för en läkare eller någon annan yrkesutbildad person inom hälso- och sjukvården att 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. I 17 kap. 16 § i rättegångsbalken föreskrivs det om en skyldighet 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 föreskrivs det att när ett meddelande enligt lagen om yttrandefrihet i masskommunikation har gjorts tillgängligt för allmänheten, får meddelandets upphovsman, utgivaren och utövaren av programverksamheten 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 utsträcks personkretsen i fråga om vissa ovannämnda vittnesförbud och rättigheter att vägra att vittna. 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. Att utsträcka hänvisningen till att omfatta 11 § 2 och 3 mom. behövs dock inte, eftersom inget förbud som avser dem inte föreslås i övrigt.

Vidare behöver det föreskrivas om åtgärder som ska vidtas, om det under tiden för avlyssning eller observation eller vid något annat tillfälle framkommer att det är fråga om ett meddelande som det är förbjudet att avlyssna eller observera. Åtgärden ska då avbrytas och de upptagningar som fåtts genom åtgärden och anteckningarna om de uppgifter som fåtts genom den genast utplånas. För tydlighetens skull bör det också föreskrivas separat om åsidosättande av förbudet när källan till ett hot är föremål för ett förbud mot avlyssning eller observation.

2.4.6.3 Utlämnande av uppgifter till andra förundersökningsmyndigheter

I lagen om militär disciplin och brottsbekämpning inom försvarsmakten finns ingen bestämmelse om utlämnande av uppgifter till andra förundersökningsmyndigheter. Den närmaste förebilden är 5 kap. 54 § i polislagen, där det föreskrivs om användning av överskottsinformation. Enligt en definition i 5 kap. 53 § i polislagen avses med överskottsinformation 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. Med andra ord kan överskottsinformation definieras som information som har fåtts som biprodukt när lagenlig informationsinhämtning har använts; den har inte varit det egentliga eller planerade syftet med åtgärderna. Regleringen om överskottsinformation bildar ett slags mellanläge mellan den möjlighet att fritt utnyttja bevisning som den fria bevisteorin medför och de inskränkningar som gäller vittnesförbud. Det kan vara fråga om information som gäller ett brott eller information som inte alls har någonting med ett brott att göra men är relevant för myndigheternas verksamhet.

Enligt 5 kap. 54 § 1 mom. i polislagen får överskottsinformation användas vid utredning av brott när informationen gäller ett sådant brott för vars förhindrande det skulle ha varit tillåtet att använda sådana metoder för inhämtande av information som har använts då informationen har fåtts. Med utredning av brott avses att avsikten är att använda information som bevisning som stöder att någon är skyldig eller som grund för ett avgörande som gäller en metod för informationsinhämtning (direkt utnyttjande) till skillnad från t.ex. avsikten att inrikta undersökningen, varvid överskottsinformation kan utnyttjas friare (indirekt utnyttjande). Inskränkningen av användningen av överskottsinformation som bevisning handlar om ett förbud mot nyttjande.

Enligt 5 kap. 54 § 4 mom. i polislagen får överskottsinformation alltid användas för förhindrande av brott, för inriktning av polisens verksamhet och som en utredning som stöder det att någon är oskyldig. Vad förhindrandet av brott beträffar gäller det att komma ihåg att detta inbegriper också avbrytande av ett fortsatt brott. Informationen kan däremot inte användas för avslöjande av brott. Informationen kan alltid användas som bevisning (bevis) som stöder det att någon är oskyldig, även om användningen de facto kan befästa att någon annan är skyldig. Enligt 5 mom. får överskottsinformation följdenligt användas också för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada. Inga ytterligare förutsättningar har angetts för användning av överskottsinformation i situationer som avses i 4 och 5 mom. i den paragraf som det är fråga om här.

Överskottsinformation uppkommer i samband med allehanda åtgärder som det hör till myndigheterna att sköta. Det är uppenbart att också användningen av metoder för underrättelseinhämtning oundvikligen kommer att resultera även i sådan information som inte hotar landets försvar eller den nationella säkerheten. I många fall bör den informationen omedelbart utplånas eftersom den är irrelevant, men en del information som saknar betydelse för landets försvar och den nationella säkerheten kan tänkas hänföra sig till ett allvarligt brott. Därför behövs reglering som styr vidareförmedlingen av information av detta slag till relevanta mottagare över huvud taget och till förundersökningsmyndigheterna i synnerhet. En norm i gränszonen mellan militär underrättelseinhämtning och straffprocessen som reglerar utlämnandet av uppgifter till förundersökningsmyndigheterna är mångfasetterad och principiellt laddad. I det skede som föregår uppfyllandet av brottsrekvisitet har syftet att förhindra brott företräde framför brottsutredningsintresset, vilket är utmärkande för förundersökningsskedet. Det är då fråga om åtgärder som dels är nödvändiga för undvikande av fara och skada, dels i regel inte kränker det centrala kärnområdet i individens rättsskydd. I domstolsskedet har det däremot i allmänhet inte ansetts att individens rättsskyddsintresse uppvägs av något starkt konkurrerande intresse. Inom den militära underrättelseinhämtningen åter prioriteras i princip syftet att skydda landets försvar och den nationella säkerheten framför intresset att förhindra och utreda brott. Militär underrättelseinhämtning handlar nämligen om åtgärder som är nödvändiga för att försvara och trygga centrala statliga eller samhälleliga intressen. Ett sådant intresse är att rättssystemet, inklusive straffprocessystemet, fungerar. Därför lämpar sig 5 kap. 54 § i polislagen sådan den lyder inte som förebild när det föreskrivs om vidarebefordran av information för att användas vid brottsbekämpning, eftersom det i paragrafen inte har beaktats att den militära underrättelseinhämtningen har ett skyddsintresse som är kopplat till landets försvar och den nationella säkerheten.

Utgångspunkt nummer ett för bestämmelsen om utlämnande av uppgifter för att användas vid brottsbekämpning är att det i den bör föreskrivas om en skyldighet att underrätta förundersökningsmyndigheten om sådana brott för vilka det föreskrivna strängaste straffet är fängelse i minst sex år. Till sådana gärningar anknyter redan ett så stort intresse att förhindra och utreda brott att det för deras del inte är kriminalpolitiskt sett acceptabelt att den information om brott som framkommit vid underrättelseinhämtning inte skulle lämnas ut till förundersökningsmyndigheterna. Det är alltså fråga om en åtgärd genom vilken man kan undvika att en allvarlig fara realiseras eller bidra till att ett grovt brott klaras upp. Följdenligt är ytterligare att uppgifter som fåtts med hjälp av en metod för underrättelseinhämtning alltid ska få lämnas ut för att ingå i en utredning som stöder det att någon är oskyldig och för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada. Dessa huvudsakligen individualistiska intressen har mycket gemensamt med de kollektiva intressen som man vill skydda genom underrättelseinhämtning. Med avseende på den i artikel 6.2 i människorättskonventionen tryggade oskuldspresumtionen bör man emellertid inta en reserverad hållning till reglering som skulle möjliggöra att uppgifter om alla brott, även obetyd-

liga, lämnas ut till förundersökningsmyndigheten. Av samma orsak gäller det att noggrant överväga också om uppgifter över huvud taget kan lämnas ut till förundersökningsmyndigheterna i kriminalunderrättelseinhämtningssyfte eller för inriktande av polisens verksamhet.

2.4.6.4 Underrättelse om informationsinhämtning

På grund av den hemliga informationsinhämtningens art accentueras rättsskyddsfrågornas betydelse både för parter och utomstående som blir föremål för sådana åtgärder och för hela det rättsliga systemets trovärdighet över huvud taget. En av de viktigaste rättsskyddsgarantierna är att en part får ta del av det material som myndigheten har. Innan parten kan göra det ska hen ha möjlighet att få veta att hemlig informationsinhämtning har använts. Partens rätt att bli underrättad är också en viktig förutsättning för en rättvis rättegång (21 § i grundlagen, artikel 6 stycke 1 i människorättskonventionen, artikel 14 stycke 1 i MP-konventionen).

En separat fråga gäller rätten att ta del av ett dokument eller en upptagning som handlar om användning av en hemlig metod för inhämtande av information. Bestämmelser om en parts rätt att ta del av en handling finns i 11 § i lagen om offentlighet i myndigheternas verksamhet. Utgångspunkten för 1 mom. i den paragrafen är att en part har rätt att hos den myndighet som behandlar eller har behandlat ärendet ta del av en myndighetshandling som kan eller har kunnat påverka behandlingen, även om handlingen inte är offentlig. I 2 mom. föreskrivs det om fall där en part, partens ombud eller partens biträde inte har den i 1 mom. avsedda rätten. Begränsningen gäller t.ex. när utlämnande av uppgifter ur handlingen skulle strida mot ett synnerligen viktigt allmänt eller enskilt intresse och när det är fråga om en handling som har upprättats i samband med förundersökning som ännu pågår, om utredningen skulle försvåras av att uppgifter lämnas ut.

Syftet med artikel 6 stycke 1 i människorättskonventionen är bl.a. att skydda parterna mot hemliga rättegångar. Jämlikheten mellan parterna (equality of arms) och principen att parterna ska höras är viktiga faktorer vid bedömningen av frågan om en rättegång som helhet betraktad ska anses vara rättvis. De 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. Jämlikhet mellan parterna förutsätter att parterna bemöts likvärdigt och opartiskt i domstolen. Också en misstänkts rätt att effektivt förbereda sitt försvar och att lägga fram motbevisning förutsätter en rätt att bli underrättad. Det bör visserligen noteras att principen om jämlikhet mellan parterna inte kränks genom att något saknas i rättegångsmaterialet. En situation där en part förfogar över eller har kännedom om en omständighet som är fördold för eller har hemlighållits för en annan part bör bedömas annorlunda. Dessutom gäller det att beakta utgångspunkten att myndigheten i rättegångsskedet inte har rätt att göra en bedömning av en uppgifts betydelse, utan det är partens uttryckliga rätt att göra det.

Med avseende på den oskuldspresumtion som uttrycks i artikel 6 stycke 2 i människorättskonventionen kan det vara betydelsefullt t.ex. att informationskällor som drivs av olika motiv inte vill eller inte är kapabla att ge objektiv information eller att de åtminstone inriktar informationsinhämtningen i överensstämmelse med sina egna motiv. Om utgångspunkten är att en informationskällas identitet inte avslöjas eller att användningen av en informationskälla inte avslöjas över huvud taget, kan informationskällans ansvar för den lämnade informationens kvalitet eller för användning av informationen inte realiseras, utan ansvaret ligger hos myndigheten.

Det finns också goda argument för alternativet att den som informationsinhämtningen riktas mot inte underrättas om åtgärden. Intressen av det slaget är åtminstone viktiga undersöknings-

relaterade orsaker. Dessutom kan det för att skydda liv och hälsa, trygga statens säkerhet och skydda sekretessbelagda taktiska och tekniska metoder vara nödvändigt att skjuta upp underrättelsen eller att avstå från den helt och hållet. När uppskovets längd bestäms kan man tänka sig en bakre gräns för hur länge brottsutredningen äventyras, medan behovet av att trygga statens säkerhet och skydda liv och hälsa kan vara långvarigare eller rentav bestående. Vid exempelvis en täckoperation avslöjar i praktiken blotta vetskapen om att metoden har använts de tidigare operationer för förhindrande eller avslöjande av brott som den som uppträtt under täckmantel har deltagit i, och följden är att den personen inte kan användas i framtiden. Dessutom kan vetskapen i värsta fall äventyra liv och hälsa för den som uppträtt under täckmantel och hens närstående. Om exempelvis både en informationskälla och en person som uppträtt under täckmantel har använts i ett sammanhang räcker det att den ena ska bli avslöjad för att liv och hälsa för båda två och deras närstående ska utsättas för fara.

Människorättsdomstolen har bl.a. 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 inte allt material avslöjas för en misstänkt, om ett motsatt intresse gäller den nationella säkerheten, skyddet för liv och hälsa eller undersökningsmetoder som ska hemlighållas. Artikel 6 stycke 1 i människorättskonventionen tillåter emellertid bara absolut nödvändiga ingripanden i den åtalades rättigheter.

I 5 kap. 58 § 1 mom. i polislagen föreskrivs det om teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, systematisk observation, förtäckt inhämtande av information, teknisk observation och kontrollerade leveranser. När dessa metoder används ska den som varit föremål för dem underrättas om detta skriftligen utan dröjsmål efter det att syftet med inhämtandet av information har nåtts. Den absoluta bakre gräns för underrättelsen som anges i 1 mom. är dock ett år efter att det hemliga inhämtandet av information har upphört. Samtidigt ska den domstol som beviljat tillståndet informeras skriftligen om underrättelsen. Underrättelsen ska specificeras med sådan noggrannhet att den som varit föremål för informationsinhämtning vid behov kan sträva efter att ta reda på grunderna för användning av den metod som använts i hens fall. Sekretessbelagda taktiska och tekniska metoder behöver inte avslöjas i underrättelsen. Om den som varit föremål för inhämtandet av information inte kan identifieras kan givetvis ingen underrättelse göras. Om personens identitet klarnar längre fram, ska underrättelsen göras i efterhand. Fastän hemliga metoder för inhämtande av information de facto riktas också mot andra personer, behöver de inte underrättas.

Bestämmelsen i 5 kap. 58 § 5 mom. i polislagen gäller systematisk observation, förtäckt inhämtande av information, täckoperationer, bevisprovokation genom köp och styrd användning av informationskällor. Huvudregeln är att den som varit föremål för en sådan metod ska underrättas om den, om förundersökning inleds i ärendet. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § i tvångsmedelslagen iakttas i tillämpliga delar. Samtidigt ska den domstol som beviljat tillståndet informeras skriftligen om underrättelsen, och för en täckoperations vidkommande informeras den domstol som avses i 32 § i tvångsmedelslagen, dvs. Helsingfors tingsrätt. Detsamma gäller bevisprovokation genom köp och styrd användning av informationskällor med stöd av 10 kap. 60 § 7 mom. i tvångsmedelslagen, varvid 43 § 6 mom. i samma kapitel ska iakttas i tillämpliga delar. Man bör lägga märke till att domstolen har en roll i beslutsprocessen endast vid täckoperationer, inte vid bevisprovokation genom köp och styrd användning av informationskällor. Trots det ska domstolen informeras skriftligen om underrättelserna till dem som varit föremål för alla dessa metoder.

I 5 kap. 58 § 2 mom. i polislagen föreskrivs det om undantag från huvudreglerna för underrättelse. Enligt momentet får 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 inhämtning av information, trygga statens säkerhet eller skydda liv eller hälsa. Den grund som gäller statens säkerhet kommer i praktiken i fråga bara inom skyddspolisens ansvarsområde. Det gäller att notera att ett beslut om att skjuta upp underrättelsen inte förpliktar till att fördröja underrättelsen ända till den utsatta dagen. Om omständigheterna förändras så att förutsättningar för att underrättelsen ska utebli inte längre finns, ska underrättelsen göras trots uppskovsbeslutet (BJO Dnr 1716/2/09 och BJO Dnr 609/2/10). Uppskovsgrunderna täcker också olika situationer där internationella samoperationer företas samt situationer där det upptäcks att föremålet för informationsinhämtning har varit fel. Ett uppskov innebär alltså att underrättelsen skjuts upp, men det är också möjligt att underrättelsen uteblir helt. Enligt det ovannämnda momentet får det beslutas att underrättelsen ska utebli, om det är nödvändigt för att trygga statens säkerhet eller skydda liv eller hälsa. Domstolen beslutar att underrättelsen ska skjutas upp eller utebli, trots att en anhållningsberättigad tjänsteman har beslutat att metoden ska användas.

Principerna för bestämmelsen i 5 kap. 58 § i polislagen om underrättelse om hemligt inhämtande av information fungerar som förebild när det föreskrivs om underrättelse om att metoder för underrättelseinhämtning har använts. Det finns skäl att överlåta åt domstolen att pröva huruvida underrättelsen bör skjutas upp respektive utebli, eftersom domstolen bäst kan bedöma de olika parternas rättigheter och behov av att bli underrättade. Med hänsyn till att regleringen i lagen om militär underrättelseverksamhet föreslås vara uppbyggd på inhämtning av information om verksamhet som är föremål för militär underrättelseinhämtning bör grunderna för att skjuta upp underrättelsen och grunderna för beslut om att underrättelsen ska utebli kompletteras med behovet att trygga landets försvar och den nationella säkerheten. Vidare bör det bedömas vilket slag av underrättelsearrangemang som är det mest adekvata med tanke på både rättsskyddet för den som en metod för underrättelseinhämtning har riktats mot och de praktiska underrättelsemöjligheterna i fråga om de nya metoder som förelås i lagen om militär underrättelseverksamhet, dvs. platsspecifik underrättelseinhämtning och kopiering. Det gäller också att beakta statliga aktörers ställning i systemet med de grundläggande fri- och rättigheterna.

### 2.4.7 Underrättelseinhämtning som avser utländska förhållanden

De förändringar som inträffat i Försvarsmaktens verksamhetsmiljö på senare år bottnar i att hoten mot Finlands yttre, interna och nationella säkerhet samt anknytande fenomen har internationaliserats i accelererande takt och samtidigt blivit allt mer it-baserade. Skiljelinjen mellan inre och yttre säkerhet har blivit mindre skarp. Den nationella och den internationella verksamhetsmiljön flätas mer och mer ihop med varandra. De allvarligaste hoten mot Finlands nationella säkerhet är så gott som utan undantag av internationellt ursprung eller har kopplingar till utlandet. Följden av detta är att inte all information som påverkar säkerheten i det finska samhället är tillgänglig inom landet. En enskild stat klarar inte i alla situationer av att enbart genom egna åtgärder avvärja hot som riktas mot den. Förändringen framhäver vikten av internationellt underrättelse- och säkerhetsarbete och av den operativa och strategiska information som fås med dess hjälp. Den operativa och strategiska internationella meddelandetrafiken inom sektorn har nästan fyrfaldigats under 2000-talet.

Till följd av arten hos underrättelseinhämtning som avser utländska förhållanden utgår verksamheten från att man strävar efter att använda en så mjuk metod som möjligt för att inhämta den information som behövs. I praktiken baserar sig underrättelseinhämtning ofta på hand-

lingsmodeller som påminner starkt om sambandsverksamhet. Det är fråga om ett utbyte av information och uppfattningar som sker på frivillig basis mellan myndigheterna i två stater och gagnar båda parterna. Informationsutbytet kan gälla t.ex. fenomen, enskilda händelser, iakttagelser eller politiska stämningar av gemensamt intresse som den part som ger informationen erbjuder sin egen tolkning av, varvid den strävar efter att påverka mottagarpartens uppfattning. Utöver sådant ömsesidigt informationsutbyte kan underrättelseinhämtning som avser utländska förhållanden grunda sig på ensidigt agerande från den stats sida som bedriver underrättelseverksamhet. I normalläget inbegriper verksamheten att personal som har sänts ut av den stat som bedriver underrättelseverksamhet gör allmänna iakttagelser av förhållandena i stationeringslandet utgående från sin tjänsteställning och för diskussioner med representanter för eller medborgare i stationeringslandet. Även om det i detta fall inte är fråga om informationsutbyte som uttryckligen har överenskommits med stationeringslandet, sker verksamheten ofta med stationeringslandets tysta godkännande. Alla länder måste de facto till en viss gräns tolerera underrättelseinhämtning på sitt territorium.

I vissa situationer som kan karaktäriseras som exceptionella räcker det inte med den ovan beskrivna underrättelseinhämtningen som betonar samarbete eller grundar sig på ett tyst godkännande. I sådana fall bör information som är ytterst viktig för Finland kunna inhämtas med hjälp av hemliga metoder för underrättelseinhämtning.

Flera europeiska stater har lagstiftat om underrättelseinhämtning som avser utländska förhållanden och om de befogenheter som får användas vid den. Bedömningen av hur pass detaljerade bestämmelser om de enskilda befogenheterna som varit motiverade varierar från land till land. Med underrättelseinhämtning som avser utländska förhållanden avses säkerhetsmyndigheternas aktiva agerande för att inhämta information om sådana enskilda eller statliga aktörer som befinner sig utomlands och som kan tänkas hota Finlands nationella säkerhet eller andra vitala samhällsintressen eller hänför sig till militär verksamhet.

*Målstatens synvinkel*

Enligt en allmän folkrättslig princip har varje suverän stat rätt till territoriell integritet och politiskt oberoende i relation till andra stater. Varje stat beslutar själv huruvida den tillåter, och på vilka villkor, att utländska tjänstemän är verksamma på dess territorium. De flesta stater tolererar de facto till en viss gräns, eller godtar rentav, att främmande underrättelsemyndigheter är verksamma på deras territorium. Det kan handla om informationsutbyte som gagnar båda parterna eller vara fråga om att informationsinsamling som en främmande stat bedriver öppet och som gäller de allmänna förhållandena i målstaten inte äventyrar målstatens eller någon annan parts intressen. Under andra förhållanden kan målstaten ställa sig negativ till en främmande stats myndigheters agerande på dess territorium. Verksamheten kan från fall till fall också uppfylla brottsrekvisitet för någon gärning som är straffbar enligt målstatens strafflagstiftning. Huruvida en verksamhet är straffbar eller inte kan, beroende på målstaten, påverkas av t.ex. vem som inhämtar information, vilken information som inhämtas och vilken metod som används vid informationsinhämtningen. De jämförda staterna har inte heller de på lagstiftningsnivå ställt som villkor för underrättelseinhämtning som avser utländska förhållanden att målstaten godtar verksamheten eller att verksamheten inte överträder målstatens lagstiftning.

Underrättelseinhämtning som avser utländska förhållanden handlar om verksamhet som förutsätts för att ett godtagbart syfte, dvs. tryggande av landets försvar eller den nationella säkerheten, ska nås. I vissa situationer kan denna verksamhet inbegripa risker. En av riskerna är att det är fråga om verksamhet som strider mot målstatens lagstiftning eller annars inte är godtag-

bar från målstatens synpunkt. Det är viktigt att vid underrättelseinhämtning som avser utländska förhållanden beakta andra staters inställning och innehållet i deras lagstiftningar, men av praktiska skäl kan beaktandet inte ske när det föreskrivs om verksamheten utan först när verksamheten inleds. Det är då fråga om att överväga huruvida den fördel som verksamheten medför är avgjort större än de risker som är förknippade med den.

*Tredje stats synvinkel*

Enligt en allmän folkrättslig princip har varje suverän stat rätt till territoriell integritet och politiskt oberoende i relation till andra stater. Detta gäller också när underrättelseinhämtning sker genom att en tredje stats territorium utnyttjas på något sätt. Vidare får en stat enligt en allmän folkrättslig princip inte tillåta att dess territorium används för gärningar som skadar eller olagligen påverkar andra stater. När en gärning bedöms tillmäts inte bara frågan om huruvida gärningen orsakar skada på egendom eller personer betydelse, utan det kan räcka att gärningen har negativa verkningar över huvud taget. Vid underrättelseinhämtning som avser utländska förhållanden och försiggår på en tredje stats territorium är det t.ex. möjligt att träffa personer som fungerar som informationskällor, alternativt kan sådana värvas. Principen om transiteringsstat kan dock inte anses lämpa sig direkt på den internationella datatrafiken, där datatrafiken normalt rör sig och routas utgående från var den inte stöter på hinder, dvs. utan att routningen fastställs på förhand.

*Underrättelseverksamhet och internationell rätt*

Enligt artikel 38 i stadgan för den internationella domstolen är den internationella rättens viktigaste källor allmänna eller speciella internationella överenskommelser, internationell sedvänja och de s.k. allmänna rättsgrundsatserna. Det har inte upprättats några internationella avtal om fredstida underrättelseverksamhet. De bestämmelser om skydd för spioner under krigstid som finns i artikel 46 i första tilläggsprotokollet till Genèvekonventionen från år 1949 har ingen betydelse för det tema som behandlas här.

Även om det i underrättelseverksamheten i princip är fråga om att kränka målstatens suveränitet, är rättslitteraturen inte enig om huruvida den internationella rätten på sedvanerättens och de allmänna rättsprincipernas nivå förhåller sig accepterande eller fördömande till underrättelseverksamhet. Det torde inte kunna anses att underrättelseverksamheten har en allmänt godkänd ställning i den internationella rätten, eftersom stater genom att konstatera att en person är persona non grata eller på annat sätt icke godtagbar upprepade gånger visar att de inte accepterar sådan verksamhet. Underrättelseverksamhet kan visserligen inte heller anses vara uttryckligt förbjuden i internationell rätt, och nästan alla stater bedriver sådan verksamhet i en eller annan form. Det är fråga om en globalt etablerad verksamhet, och de enskilda staternas förhållningssätt till den bestäms av om de i respektive fall bedriver underrättelseverksamhet eller är föremål för den.

I underrättelseverksamheten har man generellt utnyttjat den immunitet och befrielse från värdlandets straffrättsliga jurisdiktion som Wienkonventionen om diplomatiska förbindelser (FördrS3-5/1970) garanterar diplomatiska representanter.

*Informationsinhämtning i samband med militär underrättelseinhämtning utomlands*

De finska säkerhetsmyndigheterna har inga lagstadgade befogenheter att inhämta information utomlands. Till följd av förändringen i säkerhetsmiljön och på de grunder som nämns i denna

proposition finns det dock behov av att föreskriva om befogenheter som gäller verksamhet utomlands, dvs. underrättelseinhämtning som avser utländska förhållanden.

Den internationella jämförelsen visar att beslutsfattandet om informationsinhämtning som sker utomlands varierar från land till land. Ansvaret för beslutsfattandet kan ligga hos t.ex. underrättelsemyndigheten själv eller hos en politiskt ansvarig part. Om underrättelsemyndigheten svarar för beslutsfattandet, sker det vanligtvis i enlighet med riktlinjer som statsledningen har dragit upp. De metoder som används vid underrättelseinhämtning riktas mot en främmande stats suveränitet i mållandet, och eventuellt också i en tredje stat via vilken informationen inhämtas. Till följd av detta framhävs den politiska dimensionen i samband med underrättelseinhämtning som avser utländska förhållanden. Underrättelseinhämtningens potentiella verkningar och risker påverkar beslutsförfarandet. Domstolarna i Finland är inte behöriga att besluta om användning av metoder utanför finskt territorium, därför kommer de inte i fråga som beslutsinstans.

2.4.8 Styrning och tillsyn

Som framgår av den internationella jämförelsen har den högsta statsledningens skyldighet att styra underrättelseverksamheten ansetts vara betydande. Styrningen kan genomföras på olika sätt, t.ex. så att den högsta statsledningen har hand om den eller genom beslut på ministernivå när förutsättningarna för att använda metoder för underrättelseinhämtning övervägs. Ett viktigt syfte med styrning av denna typ är att synpunkter som förvaltningsområden som är viktiga för underrättelseverksamheten har blir beaktade i underrättelseverksamheten i form av allmänna riktlinjer.

Förvaltningskulturen i Finland är sådan att det inte har ansetts vara möjligt för politiska beslutsfattare att delta konkret i det operativa beslutsfattandet. Styrning som den militära underrättelseverksamheten förutsätter kan ges av statsrådets utrikes- och säkerhetspolitiska ministerutskotts sammanträde med republikens president. Enligt 24 § i lagen om statsrådet (175/2003) kan ministerutskottet för utrikes- och säkerhetspolitiska ärenden sammanträda med republikens president. Republikens president eller statsministern kan ta initiativ till ett gemensamt sammanträde. Enligt 25 § 3 mom. i reglementet för statsrådet ska i utrikes- och säkerhetspolitiska utskottet förberedelsevis behandlas viktiga ärenden som gäller utrikes- och säkerhetspolitiken och viktiga ärenden av annat slag vilka gäller Finlands relationer till främmande makter, viktiga ärenden gällande den inre säkerheten i anslutning därtill samt viktiga ärenden som gäller totalförsvaret. Utskottet behandlar också frågor som gäller samordningen av ärenden som hör till dess uppgiftsområde.

Försvarsmaktens nuvarande befogenheter är sådana att Försvarsmakten inte klarar av att i tillräcklig utsträckning och effektivt producera tillförlitlig och rättidig information till stöd för den högsta statsledningens och militärledningens beslutsfattande. För att den högsta statsledningen ska få bättre tillgång till information med hjälp av militär underrättelseinhämtning förutsätts det också att den högsta statsledningen är tillräckligt medveten om underrättelseverksamheten och dess potentiella följder för Finlands internationella relationer.

Utrikes- och säkerhetspolitiska ministerutskottets sammanträde med republikens president kan redan med stöd av gällande reglering förberedelsevis behandla viktiga ärenden som gäller underrättelseverksamhet. I rådande rättsläge har den högsta statsledningen emellertid inte någon entydig rättsgrund för styrning av den militära underrättelseverksamheten.

Också aspekter som anknyter till annat än rättslig övervakning förutsätter tillräcklig reglering om styrningen av och tillsynen över den militära underrättelseverksamheten i och med att den militära underrättelseinhämtningens effekter ökar.

2.4.9 Rättslig övervakning och rättsskydd

De hemliga metoder för inhämtande av information som försvarsmakten använder övervakas av försvarsmaktens ledning, enligt 127 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Dessutom övervakar avdelningschefen för underrättelseavdelningen förebyggandet och avslöjandet av brott enligt 86 §.

Den övervakning som riksdagens justitieombudsman utför i fråga om hemliga metoder för inhämtande av information grundar sig i huvudsak på inspektioner och annan granskning som justitieombudsmannen utför på eget initiativ. Klagomål över användningen av hemliga metoder för inhämtande av information anförs endast i liten utsträckning. Justitieombudsmannen ger årligen till riksdagen en berättelse om sin verksamhet samt om tillståndet inom rättskipningen och de brister i lagstiftningen som justitieombudsmannen har observerat.

Vad skyddspolisen beträffar har grundlagsutskottet förutsatt att ett särskilt avsnitt om användningen av teletvångsmedel och täckoperationer ska ingå i berättelsen (GrUB 15/2002 rd).

Grundlagsutskottet har ett flertal gånger (GrUB 8/2007 rd, GrUB 17/2006 rd och GrUB 16/2006 rd) konstaterat att justitieombudsmannen har spelat en viktig roll när det gällt att övervaka teletvångsmedlen och utveckla övervakningssystemen. Men justitieombudsmannens laglighetsövervakning kan enligt utskottet 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 i justitieombudsmannens berättelse för 2014 bedömdes det att årliga rapporter från olika myndigheter förbättrar möjligheterna att på ett allmänt plan följa upp användningen av hemligt inhämtande av information. I konkreta fall kan justitieombudsmannens särskilda övervakning dock på sin höjd vara stickprovsmässig. I berättelsen konstateras det att justitieombudsmannens övervakning närmast bara är ett komplement till myndigheternas interna laglighetskontroll och kan karaktäriseras som kontroll av kontrollen.

I och med de nya befogenheterna bör det finnas ett heltäckande övervakningssystem för den militära underrättelseinhämtningen, med tillräckliga befogenheter att utföra övervakningen som sig bör. Övervakningssystemet bör uppfylla kraven på en effektiv och oberoende övervakning. Också människorättsdomstolen har dessutom uppmärksammat övervakningssystemen för hemliga metoder för inhämtande av information. Ett effektivt övervakningssystem består av dels parlamentarisk övervakning, dels myndighetsövervakning som står för laglighetsövervakningen. i Finland finns det för närvarande ingen myndighet med tillräckliga befogenheter att övervaka underrättelseverksamheten effektivt, oberoende och trovärdigt samt att eventuellt avbryta underrättelseverksamheten i sådana fall där missbruk förekommer. Det är orsaken till att det är ändamålsenligt att föreskriva om övervakningen i en separat lag.

Som framgår av den internationella jämförelsen gäller det att se till att regleringen om underrättelseverksamhet innefattar tillräckliga rättsskyddsarrangemang. För att underrättelseverksamhet ska vara möjlig bör underrättelselagstiftningen fylla de kriterier som t.ex. människo-

rättsdomstolen och EU-domstolen har ställt upp i sin respektive avgörandepraxis. För att rättsskyddet ska tillgodoses behöver fysiska personer ha tillgång till instrument som är tillräckliga för att deras ärende ska prövas effektivt av den behöriga myndigheten. Likaså bör föremålet för informationsinhämtningen under vissa förutsättningar underrättas om att hen varit föremål för hemlig informationsinhämtning från myndighetshåll.

2.4.10 Utlämnande av uppgifter samt internationellt samarbete

Det är nödvändigt att föreskriva på lagnivå om utlämnande av underrättelseuppgifter mellan myndigheter. För tillfället finns bestämmelser om utlämnande av uppgifter i bl.a. personuppgiftslagen, offentlighetslagen, lagen om militär disciplin och brottsbekämpning inom försvarsmakten och lagen om internationella förpliktelser som gäller informationssäkerhet. Nuläget kan ändå inte anses vara tillräckligt, eftersom underrättelseinhämtning i princip utförs för att förebygga allvarliga hot, varvid det inte är fråga om brottsbekämpning. I situationer där en händelse som är att betrakta som brott framkommer under tiden för underrättelseverksamhet kan saken enligt förslaget i vissa fall anmälas till den brottsbekämpande myndigheten eller förundersökningsmyndigheten. Enligt gällande lagstiftning kan underrättelseuppgifter som har inhämtats med hemliga metoder för inhämtande av information inte heller lämnas ut till privata parter.

Enligt nuvarande lagstiftning är internationellt samarbete kring militär underrättelseinhämtning inte möjligt i den utsträckning som anses vara behövlig. Utan en uttrycklig bestämmelse på lagnivå kan militärunderrättelsemyndigheten inte genomföra underrättelseoperationer i samarbete med internationella partner, om sådan verksamhet skulle anses behövlig med tanke på Finlands nationella intressen.

2.4.11 Reservisters deltagande i militär underrättelseinhämtning

På grund av reservisternas höga kompetensnivå bör det vara möjligt att vid behov använda reservister i militär underrättelseverksamhet. I dagsläget kan reservister användas i sådana uppgifter inom den militära underrättelseinhämtningen där det inte krävs lagstadgade befogenheter. Reservister kan också kallas till repetitionsövningar i samband med en flexibel höjning av den militära beredskapen.

Vid informationsinhämtning som avses i lagen om militär disciplin och brottsbekämpning inom försvarsmakten kan reservister användas när republikens president i enlighet med 83 § i värnpliktslagen har beslutat om extra tjänstgöring.

Bland reservisterna finns också personer som har varit tvungna att avgå från militärunderrättelsemyndighetens tjänst på grund av den pensionsålder som tillämpas inom Försvarsmakten. Det innebär att det till reserven hör personer med avsevärd kompetens inom underrättelsesektorn som har utövat befogenheter samt beslutat om befogenhetsutövning.

Militärunderrättelsemyndigheten kan dock också under normala förhållanden bli tvungen att inhämta mer underrättelseuppgifter än vanligt om förändringar i omvärlden och om lägesutvecklingen. Det bör därför vara möjligt att använda reservister framför allt i en situation där Försvarsmaktens beredskap effektiviseras i och med förändringar i verksamhetsmiljön. Reservister kan kallas till repetitionsövningar omedelbart, om ett nödvändigt behov av det framkommer i Finlands säkerhetsmiljö.

Användningen av reservister är till väsentliga delar också kopplad till militär krishantering och givande av internationellt bistånd. Finlands deltagande i insatser av det slaget stöder sig till stor del på reservister som fått särskild utbildning för dem. Med undantag för underrättelseverksamhet med anknytning till skydd av egna styrkor på krishanteringsområden har det inte föreskrivits om särskilda befogenheter för reservister att inhämta information i samband med krishantering och internationellt bistånd.

Användningen av reservister i Finland samt vid krishanteringsinsatser och internationellt bistånd förutsätter bestämmelser om befogenheter, övervakning och styrning, reservisternas straffrättsliga ansvar och skadeståndsskyldighet samt en noggrann avgränsning i fråga om metoderna för underrättelseinhämtning och behandlingen av information. Reservisternas verksamhet bör inte heller inbegripa utövning av offentlig makt.

2.4.12 Organisationernas möjlighet att gardera sig mot hot mot informationssäkerheten

De sabotageprogram som är svårast att upptäcka och samtidigt skadar den nationella säkerheten mest är statliga spionprogram och andra sabotageprogram. Signaturerna för sådana sabotageprogram är information som omfattas av hög skyddsnivå och som i typiska fall utbyts i det internationella samarbete som säkerhets- och underrättelsetjänsterna bedriver. Eftersom Kommunikationsverket varken är eller kan vara part i detta konfidentiella samarbete är det inte möjligt att lämna ut till Havaro-systemet sådana identifikationer som har den största betydelsen med tanke på skyddet av den nationella säkerheten.

De åtgärder för informationssäkerheten som möjliggörs i 272 § i informationssamhällsbalken, Havaro medräknad, syftar till att genomföra informationssäkerheten genom att skydda enskilda organisationer mot kränkningar som riktas mot dem. Syftet med åtgärderna för informationssäkerheten är inte att täcka informationsbehov med anknytning till upptäckande och bekämpning av verksamhet som äventyrar den nationella säkerheten. För den som vidtar åtgärder för informationssäkerheten är information som är väsentlig för upprätthållande av den nationella säkerheten, t.ex. orsakerna till de allvarligaste kränkningarna av informationssäkerheten, omständigheterna kring kränkningarna, förövarna och bakgrundsmotiven, inte central. Det är ändamålsenligt att information om hot mot och kränkningar av informationssäkerheten som är betydande med tanke på den nationella säkerheten kan lämnas ut mellan olika aktörer.

2.4.13 Sammanfattning av bedömningen av nuläget

Den högsta statsledningen i Finland har uppmärksammat behovet av underrättelselagstiftning. Republikens president och statsrådets utrikes- och säkerhetspolitiska ministerutskott tog i november 2013 ställning för att arbetet med att utveckla lagstiftningen skulle påbörjas genast som ett inslag i genomförandet av Finlands cybersäkerhetsstrategi.

Enligt programmet för statsminister Juha Sipiläs regering kräver de ökande riskerna och nya hoten beredskap och förberedelser av ett nytt slag av hela samhället. Detta gäller framför allt nya och omfattande hot som påverkansåtgärder av hybridkaraktär, cyberattacker och bekämpning av terrorism. Syftet med Försvarsmaktens system för militär underrättelseinhämtning är att förhandsvarna statsledningen om utvecklingen av militära hot, vilket möjliggör att statsledningen fattar rättidiga beslut och leder de vitala samhällsfunktionerna. Den information som är central för den militära underrättelseinhämtningen har i betydande utsträckning övergått från analoga kanaler till digitala, och för närvarande saknar den militära underrättelseinhämtningen befogenheter att använda dem som källor för informationsinhämtning. För att förändringarna ska kunna anammas förutsätts det att lagstiftningen ses över så att de myndigheter som ansva-

rar för den nationella säkerheten klarar av att sköta sina lagstadgade uppgifter tillräckligt effektivt. Med hänsyn till grundlagens bestämmelser går det inte längre att betrakta som acceptabelt att hänvisningar till militär underrättelseinhämtning finns enbart i förarbetena till lagen om försvarsmakten och att den militära underrättelseinhämtningen regleras i Försvarsmaktens interna normer.

Försvarsmaktens uppgifter går ut på att avvärja hot mot landets försvar och den nationella säkerheten. Avvärjningen av hot förutsätter att man tillräckligt tidigt kan upptäcka hoten och få information om dem. För att det ska vara möjligt att gardera sig mot att hoten förverkligas gäller det att få information om dem i ett tillräckligt tidigt skede.

Det finns inte några bestämmelser om behörigheten i fråga om underrättelseinhämtning för de myndigheter som avvärjer militära hot och hot mot den nationella säkerheten och om fördelningen av denna behörighet mellan de militära och de civila myndigheterna. I gällande reglering grundar sig myndigheternas befogenheter att inhämta information uteslutande på brottsbekämpning i stället för på underrättelseverksamhet.

De osäkerhetsfaktorer som hör samman med den förändrade säkerhetsmiljön betonar behovet av att producera oberoende, verifierad och analyserad information om hoten mot Finlands säkerhet till stöd för både det politiska beslutsfattandet och säkerhetsmyndigheternas beslutsfattande. En tillräcklig förmåga att komma med förhandsvarningar kan garanteras endast om sanningsenlig information om vilka avsikter de som ligger bakom hot har och vad de planerar fås i ett så tidigt skede som möjligt. Tillgång till information på ett tidigt stadium förbättrar det finska samhällets möjligheter att gardera sig mot hot och breddar urvalet av medel med vars hjälp man kan förhindra att hoten verkställs. Också med tanke på förberedelserna för undantagsförhållanden är det nödvändigt att man redan under normala förhållanden kan inhämta information om militära hot som riktas mot Finland.

Det kan anses att de hemliga metoderna för inhämtande av information leder till information om föremålen för militär underrättelseinhämtning, varvid det gäller att ändra endast syftet med och förutsättningarna för att utöva befogenheter. Genom t.ex. teleavlyssning går det att få detaljerad information om en person. Den verksamhet som är föremål för informationsinhämtning är inte nödvändigtvis straffbar enligt lag eller så långt hunnen att den skulle kunna bli föremål för en konkret och specificerad brottsmisstanke. För närvarande är teleavlyssning inom ramen för militär underrättelseinhämtning emellertid inte möjlig ens på brottsrelaterade grunder.

Genom befogenheter att bekämpa brott kan man täcka bara en liten del av den militära underrättelseinhämtningens verksamhetsmiljö. Befogenheterna enligt lagen om militär disciplin och brottsbekämpning inom försvarsmakten är begränsade, och med hjälp av dem kan behövlig information inhämtas bara om en liten del av säkerhetsmiljön. innanför Finlands gränser. Effektiv militär underrättelseverksamhet kräver att den som bedriver verksamheten får tillgång till mer omfattande metoder för informationsinhämtning än lagen om militär disciplin och brottsbekämpning inom försvarsmakten för närvarande möjliggör. För att behövlig information om hot ska fås gäller det att kunna inhämta information t.ex. hos personer som inte hör till en finsk myndighet och genom täckoperationer samt via datanät.

På grund av att befogenheter saknas eller befogenheterna är begränsade är det möjligt att Försvarsmakten inte är kapabel att i tillräckligt god tid upptäcka sådana hot mot Finland eller mot sin verksamhet som skulle kunna äventyra försvarets säkerhet eller systemets prestanda. De

tillgängliga befogenheterna ger inte till alla delar möjlighet att tidsenligt svara på förändringar i en operativ aktörs praktiska handlingsmodeller.

Det har i många sammanhang ansetts att Finlands attraktionskraft som investeringsobjekt grundar sig på rena datanät och på Finlands rykte som ett land där datasekretessen ligger på en hög nivå. Bedömningen att datanäten är rena ifrågasätts i en rapport från Cybersäkerhetscentret, enligt vilken det i de västländer som systematiskt bevakar cyberattacker årligen upptäcks tiotals fall av cyberspionage där riktade sabotageprogram har använts som tekniska hjälpmedel. Enligt rapporten gäller hotet också Finland. Till skillnad från dessa länder har Finland i dagens läge inget system med vars hjälp särskilt allvarliga riktade attacker från sabotageprogram skulle kunna bevakas. Därför kan det bedömas att uppfattningen om särskilt rena datanät åtminstone i fråga om de allvarligaste cyberdåden grundar sig på bristfällig nationell förmåga att upptäcka sådana dåd.

Nuläget kan anses vara otillfredsställande, när man beaktar de förändringar som har skett i säkerhetsmiljön. Det bör säkerställas att det finska samhället kan fungera också vid särskilt allvarliga yttre hot samt dåd som riktar sig mot kritisk infrastruktur. Det som är centralt med tanke på den nationella säkerheten är att information om förändringar som sker i Finlands säkerhetsmiljö fås på ett tillräckligt tidigt stadium, inte att det inhämtas information som syftar till att förundersökning ska kunna genomföras.

Utgående från den internationella utvecklingen kan man notera att digitaliseringen och den omständigheten att en allt större del av kommunikationen sker via datanät märks i många olika staters lagstiftning. I flera stater pågår arbete med att bereda ändringar i lagstiftningen om underrättelseinhämtning, och i vissa stater har ändringarna redan trätt i kraft. Olika staters lagstiftningsprojekt har påskyndats av bl.a. människorättsdomstolens och EU-domstolens avgörandepraxis på senare tid som hänfört sig till detta. I människorättsdomstolens och EU-domstolens avgöranden har respekten för privatlivet och vikten av de grundläggande rättigheter som gäller skyddet för personuppgifter betonats, särskilt i samband med elektronisk kommunikation. Det kan visserligen anses att människorättsdomstolen och EU-domstolen betraktar statens säkerhetsintresse som en grund som begränsar de grundläggande och mänskliga rättigheterna.

En förutsättning för att hoten ska kunna avstyras på ett framgångsrikt sätt är att myndigheterna med ansvar för den nationella säkerheten så tidigt som möjligt får kännedom om sådana kontakter och det som behandlas inom ramen för dem och som äventyrar den nationella säkerheten. Tillgång till information på ett tidigt stadium förbättrar det finska samhällets förmåga att reagera och breddar därmed det metodutbud med hjälp av vilket man kan förhindra att hoten realiseras eller förbereda sig på det. Den informationsinhämtning som de myndigheter som svarar för den nationella säkerheten riktar mot kommunikationen i datanät har globalt sett innehaft en central ställning t.ex. vid förhindrande av terrordåd. Nya befogenheter som förbättrar tillgången till information och möjligheterna att vidta förberedelser förutsätter ny reglering i fråga om personbaserad underrättelseinhämtning, underrättelseinhämtning som avser datasystem, radiosignalspaning och underrättelseinhämtning som avser datatrafik.

## 3 Målsättning och de viktigaste förslagen

### 3.1 Målsättning

Målsättningen för lagstiftningsprojektet är att bereda centrala bestämmelser om den militära underrättelseinhämtningen och modernisera de befogenheter till underrättelseinhämtning som

myndigheterna inom Försvarsmakten har. Det övergripande målet är att förbättra samhällets säkerhet.

Finlands yttre säkerhetsmiljö utvecklas i allt snabbare takt. I den förändring av verksamhetsmiljön som orsakats av bl.a. hybridpåverkan och digitaliseringen behöver Finland bättre än tidigare kunna inhämta information också om händelser på fenomennivå och hotbaserad information. Lagstiftningen behöver utvecklas så att den motsvarar den förändrade verksamhetsmiljön. Med de nuvarande befogenheterna att bekämpa brott går det inte att tillräckligt effektivt och tidigt upptäcka hot mot finska staten och det finska samhällets säkerhet, och inte heller att utifrån inhämtad information om hoten vidta sådana åtgärder som hoten förutsätter. Spridning och användning av falsk information accentuerar säkerhetsmyndigheternas behov av att producera objektiv, verifierad och analyserad information till stöd för den högsta statsledningens beslutsfattande. Därför bör rättsgrunden för underrättelsemyndigheternas informationsinhämtning utvecklas.

Befogenheterna till underrättelseinhämtning utgör en helhet av olika metoder för underrättelseinhämtning som kompletterar varandra. Som framgår av den internationella jämförelsen förfogar de statliga underrättelsemyndigheterna över likartade befogenheter till underrättelseinhämtning som enligt lagstiftningen i Finland får användas bara för brottsbekämpning. De sistnämnda befogenheterna inbringar inte tillräckligt med information för tryggande av samhällets säkerhet, utan det är nödvändigt att inhämta och verifiera informationen med hjälp av olika metoder för underrättelseinhämtning som stöder varandra.

Arbetsgruppen för en informationsanskaffningslag föreslog i sitt betänkande att det i Finland ska skapas en rättsgrund för underrättelseinhämtning som avser datatrafik, personbaserad underrättelseinhämtning som avser utländska förhållanden och underrättelseinhämtning som avser utländska datasystem. Dessutom är det enligt arbetsgruppen nödvändigt, av samma orsaker som gäller underrättelseinhämtning som avser utländska förhållanden, att skapa en rättsgrund för sådana befogenheter till underrättelseinhämtning som är avsedda att utövas i Finland. Underrättelsemetoderna ersätter inte varandra, eftersom de delvis är olika till sin art. Syftet med underrättelseinhämtning som avser datatrafik är framför allt att upptäcka hot som äventyrar samhällets säkerhet. Avsikten är att det genom personbaserad underrättelseinhämtning och underrättelseinhämtning som avser datasystem huvudsakligen ska inhämtas information om sådana hot och sådan verksamhet som redan har identifierats.

Det finns inte uttryckliga lagbestämmelser om informationsinhämtning som Försvarsmakten utför genom underrättelseinhämtning, alltså militär underrättelseinhämtning. Enligt förarbetena till lagen om försvarsmakten är produktion av information en del av försvarsmaktens uppgifter, men några egentliga befogenheter som avser detta ingår inte i lagen. Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag. Enligt grundlagens 119 § ska de allmänna grunderna för statsförvaltningens organ regleras genom lag, om deras uppgifter omfattar utövning av offentlig makt.

Dessutom gäller det att fästa vikt vid säkerhetsmyndigheternas befogenhetsutövning och förutsättningarna för att utöva befogenheterna, medborgarnas rättsskydd och frågor som tangerar de grundläggande fri- och rättigheterna. När bestämmelser om säkerhetsmyndigheternas befogenhetsutövning utarbetas är det nödvändigt att ta hänsyn till människorättsdomstolens och EU-domstolens avgöranden samt andra internationella förpliktelser och att beakta att de grundläggande och mänskliga rättigheterna är i fokus för t.ex. människorättskonventionen.

Meningen är att det i lagen ska föreskrivas exakt och heltäckande om befogenheterna för de parter som sköter Försvarsmaktens militära underrättelseinhämtning, så att såväl skyddet för de grundläggande och mänskliga rättigheterna som den militära underrättelseinhämtningens behov blir beaktade. Bestämmelser om behandlingen av personuppgifter föreslås bli placerade i en separat lag. Likaså föreslås det bli föreskrivet om en skyldighet för Försvarsmakten att fungera som teknisk genomförare av underrättelseverksamhet som den civila underrättelsemyndigheten bedriver. Grundlagsutskottet har ansett att vid lagstiftning om undantagsförhållanden kan begränsningar i delegeringen av lagstiftningsbehörighet i princip inte bedömas mer generöst än vid annan lagstiftning, eftersom den möjligheten inte explicit nämns i grundlagen (GrUU 6/2009 rd).

Avsikten är att genom lagstiftning om militär underrättelseinhämtning avhjälpa den i många hänseenden bristfälliga situation som för närvarande utgör en belastning för underrättelseverksamheten och att samtidigt se till att den finska lagstiftningen om underrättelseinhämtning börjar motsvara den allmäneuropeiska nivån. Målet för propositionen är att förbättra Försvarsmaktens inhämtning av information om allvarliga internationella hot som anknyter till Försvarsmaktens uppgifter och inhämtning av annan information som är av betydelse för beredskapen, så att Försvarsmakten får befogenheter att utföra personbaserad underrättelseinhämtning och underrättelseinhämtning som avser datasystem samt underrättelseinhämtning som avser datatrafik. Likaså är det meningen att lagstiftningen om militär underrättelseverksamhet ska möjliggöra informationsinhämtning vid internationellt samarbete som avses i Europeiska unionens klausul om skyldighet till ömsesidigt stöd och bistånd och vid militära krishanteringsinsatser, för att på så sätt förbättra säkerheten för finländare som tjänstgör utomlands.

Propositionen innehåller bestämmelser om bl.a. syftet med Försvarsmaktens underrättelseinhämtning, om de behöriga myndigheterna samt deras uppgifter och befogenheter, om styrningen och övervakningen, om behandlingen av uppgifter och om myndighetssamarbetet. Det har omsorgsfullt kontrollerats att de föreslagna bestämmelserna är förenliga med grundlagen. Särskilt grundlagens 10 §, enligt vilken vars och ens privatliv, heder och hemfrid är tryggade, har varit central från beredningssynpunkt.

I 10 § 3 mom. i grundlagen föreskrivs det om förtrolig kommunikation. På gång är en ändring av grundlagens 10 § som föreslås tillåta att det ingrips i hemligheten för förtroliga meddelanden när militär verksamhet och den nationella säkerheten förutsätter detta.

Vid beredningen av propositionen har särskild vikt fästs vid de internationella människorättskonventioner som är förpliktande för Finland och vid människorättsdomstolens och EU-domstolens avgörandepraxis.

## 3.2 Alternativ

### 3.2.1. Bevarande av nuläget och nykriminaliseringar

I alternativet att nuläget består har Finland inte möjligheter att i förväg få information om militära hot som riktas mot staten eller om hot som allvarligt äventyrar den nationella säkerheten. I detta alternativ är informationsinhämtning möjlig endast när den är brottsrelaterad och sker innanför Finlands gränser eller när sådana metoder för underrättelseinhämtning som inte anses förutsätta en separat rättsgrund används.

Informationen om händelser utomlands och om utländska förhållanden baserar sig i detta alternativ på uppgifter som myndigheterna i andra stater meddelar frivilligt. Dessutom är det i

det internationella samarbetet inte nödvändigtvis möjligt att få all behövlig information därför att Finland inte kan hjälpa andra stater med underrättelseverksamhet. Underrättelseuppgifter kan inhämtas såväl i som utanför Finland, antingen avgiftsfritt eller mot en avgift, ur källor som är offentliga eller annars fritt tillgängliga.

Som framgår av nulägesbeskrivningen och nulägesanalysen rör sig en stor del av kommunikationen numera annanstans än via radiovågor eller i ett telesystem. Om nuläget består är det inte möjligt att inrikta informationsinhämtningen effektivt på kommunikationen i datanät. Med stöd av dagens brottsrelaterade befogenheter, t.ex. teleavlyssning, går det inte att få information ur utländsk datatrafik eller i fråga om ett meddelande som härrör från en stat utanför Finland och går via Finland och vars destination är en annan stat än Finland.

Vid sidan av alternativet att nuläget består har det föreslagits att möjligheten att utvidga brottsbekämpningsbefogenheternas användningsområde bör övervägas. Utan att lagstiftning om underrättelseverksamhet skapas är det möjligt att överväga också att det föreskrivs om vissa nykriminaliseringar och om att området för förberedelse till brott utsträcks så långt att de nuvarande befogenheter som det föreskrivs om i lagen om militär disciplin och brottsbekämpning inom försvarsmakten och polislagen kan utövas för att greppa vissa händelseutvecklingar som definieras som brott. Denna lösning skulle kunna möjliggöras t.ex. genom att förehavanden som äventyrar stats- eller samhällsordningen kriminaliseras, såvida de nu inte omfattas av strafflagen, och genom att det materiella eller geografiska tillämpningsområdet för de tvångsmedel som Försvarsmakten har tillgång till breddas. Detta inbegriper ändå inte underrättelseverksamheten, där de händelser som är föremål för informationsinhämtning inte är några brott eller aldrig skulle komma att utgöra brott. Dessutom utgör den finska strafflagens geografiska tillämpningsområde ett hinder i fråga om verksamhet som äger rum utomlands.

Nykriminaliseringar är problematiska med tanke på den straffrättsliga legalitetsprincipen, som det föreskrivs om i 8 § i grundlagen. Strafflagstiftningen är på samma sätt som lagstiftningen i övrigt föremål för begränsningar som härrör från grundlagen och sådana internationella människorättsförpliktelser som är bindande för Finland. De grundläggande fri- och rättigheterna begränsar vilka gärningar det kan föreskrivas om straff för och hurdana straff och andra påföljder som kan förenas med brott. Genom lag kan det t.ex. inte föreskrivas att sådana åtgärder som grundlagen uttryckligen berättigar till ska vara straffbara (GrUU 17/2006 rd, GrUU 20/2002 rd, GrUU 33/2000 rd, GrUU 6/1998 rd, GrUU 23/1997 rd).

Vid nya kriminaliseringar och när kriminaliseringar utsträcks gäller det också att notera att kriminaliseringar i rättssystemet alltid är att betrakta som ultima ratio, alltså en sista utväg.

Eftersom en begränsning av de grundläggande fri- och rättigheterna måste vara acceptabel kräver kriminaliseringar ett vägande samhälleligt behov och en grund som kan godtas med hänsyn till systemet för de grundläggande fri- och rättigheterna. Exempelvis kan skyldigheten att skydda en grundläggande fri- eller rättighet vara en godtagbar grund för kriminalisering (GrUU 23/1997 rd). Visserligen har grundlagsutskottet i praktiken förhållit sig avvisande exempelvis till kriminaliseringar som föreslagits av rent symboliska skäl (GrUU 5/2009 rd, GrUU 26/2004 rd, GrUU 20/2002 rd, GrUU 29/2001 rd).

Den straffrättsliga legalitetsprincipen innefattar ett särskilt krav på exakthet i lag. Brottsrekvisitet för varje brott ska därmed anges tillräckligt exakt i lag så att det utifrån lagens lydelse går att förutse om en viss handling eller försummelse är straffbar (se t.ex. GrUU 38/2012 rd, GrUU 68/2010 rd, GrUU 58/2010 rd, GrUU 33/2010 rd, GrUU 12/2010 rd, GrUU 17/2006 rd).

Längre fram i denna proposition behandlas verksamhet som är föremål för militär underrättelseinhämtning. Ovan i propositionen har det också konstaterats att det existerar hot som inte skulle kunna framskrida till brott, t.ex. militär verksamhet som riktas mot Finland utifrån. Så långt gående eller så vaga kriminaliseringar skulle vara problematiska med tanke på den straffrättsliga legalitetsprincipen. På så sätt skulle det bli nödvändigt att utesluta sådana grunder för utövning av befogenheter till underrättelseinhämtning som är synnerligen viktiga för Finlands nationella säkerhet och för vars del de händelser som är föremål för informationsinhämtning inte skulle vara brott eller aldrig skulle komma att bli brott. Dessutom utgör den finska strafflagens geografiska tillämpningsområde ett hinder när det gäller verksamhet utomlands.

En förutsättning för de hemliga metoder för inhämtande av information som det föreskrivs om i 5 kap. i polislagen är att användningen av dem är knuten till ett visst brott. Utfärdandet av bestämmelser om användningsförutsättningarna föregicks av en enhetlig granskning av de värderingar som kan främjas och skyddas genom strafflagen samt en bedömning av behovet av att föreskriva om straff för olika gärningar. Det kan inte anses vara befogat att föreskriva om nykriminaliseringar som är inexakta från den straffrättsliga legalitetsprincipens synpunkt för att brottsrelaterade befogenheter ska kunna utövas i underrättelseverksamheten.

Straffskalorna för brott måste utformas och motiveras utifrån straffvärdet för varje enskild typ av gärning. Straffskalorna avgörs inte utgående från hur bestämmelserna om hemliga metoder för inhämtande av information kan tillämpas på ett brott eller vilken inverkan ett föreskrivet straff har på preskriptionen av brott. Vilket maximistraff användningen av en hemlig metod för inhämtning av information är knuten till har övervägts skilt för sig för varje informationsinhämtningsmetods del. De hemliga metoderna för inhämtning av information kan inte systematiseras som kraftiga respektive lindriga utgående från hur allvarliga brott som förutsätts för att en viss metod för informationsinhämtning ska kunna användas. Ur strafflagstiftningens synvinkel är de befogenheter med stöd av vilka brott förhindras, avslöjas och reds ut relevanta, men bestämmandet av straffmaximum för ett visst brott får enligt allmän lagstiftningspraxis inte grunda sig på att straffmaximum används för eventuella framtida befogenheter utan på hur klandervärda gärningarna är. Med andra ord ska beslut om straffskalorna för förberedelsebrott fattas i enlighet med proportionalitetsprincipen, och stränga skalor kan inte motiveras med befogenheter eller avsaknad av dem. Teleavlyssning kan användas endast vid undersökning av mycket allvarliga brott, och dessa brott är uppräknade i lag.

En annan framträdande brist som gäller möjligheten att tillämpa brottsrelaterade befogenheter på underrättelseverksamhet är att sådana befogenheter kan avse bara en viss person som kan specificeras och som på goda grunder kan antas komma att göra sig eller redan ha gjort sig skyldig till ett brott av en viss allvarlighetsgrad eller förberedelse till ett sådant. Om det inte föreligger en sådan brottsrelaterad grund i samband med en viss person, är det inte möjligt att använda en hemlig metod för inhämtande av information i enlighet med polislagen. Dessutom skulle teleavlyssning och teleövervakning också i underrättelseinhämtningssyfte med stöd av ett tillstånd som domstolen beviljar kunna inriktas bara på kommunikation som vissa specificerade personer bedriver och på de abonnemang eller anordningar som de innehar, inte på datatrafik med hjälp av vissa specificerade sökbegrepp.

En tredje omständighet som behöver beaktas är att underrättelseinhämtning som avser datatrafik skulle inriktas på datatrafik som överskrider Finlands gränser, i princip alltså utländsk kommunikation. Merparten av de länder dit Finlands nuvarande och planerade datakommunikationsförbindelser går kan redan nu med stöd av sin egen lagstiftning ge akt på datatrafik som går genom deras territorium. Underrättelseinhämtning som avser datatrafik har möjlig-

gjorts genom lagstiftning åtminstone i Sverige, Tyskland och Ryssland. Dessutom har det i Norge getts ett betänkande om utveckling av underrättelseinhämtning som avser datatrafik. Detta innebär att den datatrafik som går via Finlands internationella nätförbindelser redan nu kan bli föremål för underrättelseinhämtning som andra myndigheter än landets egna utför.

Det ovan angivna alternativet att utsträcka de nuvarande brottsrelaterade befogenheternas materiella och geografiska tillämpningsområde har inte vunnit understöd, eftersom det inte alls är möjligt att använda de nuvarande metoderna för inhämtande av information när det gäller att upptäcka hot som tills vidare är okända och att identifiera hotkällorna. Detta behandlades redan ovan i allmänna motiveringen. Inriktandet av denna typ av underrättelseinhämtning som avser datatrafik förutsätter också att uppgifter om teleadressen eller teleterminalutrustningen är kända i förväg. Modellen förutsätter även att det föreskrivs om omfattande skyldigheter för de centrala datatrafikaktörerna, teleoperatörerna, att bevara och lämna ut uppgifter.

Nya och utvidgade kriminaliseringar skulle ändå inte lösa problemet att Försvarsmakten med stöd av lagen om militär disciplin och brottsbekämpning inom försvarsmakten har endast begränsade befogenheter att inhämta information. Försvarsmakten skulle inte klara av att inhämta heltäckande information t.ex. hos informationskällor genom teleavlyssning eller förtäckt inhämtande av information eller i datanät genom underrättelseinhämtning som avser datatrafik eller i vissa datasystem genom underrättelseinhämtning som avser datasystem. Heltäckande militär underrättelseinhämtning skulle förutsätta att det i lagen om militär disciplin och brottsbekämpning inom försvarsmakten tas in bestämmelser om nya befogenheter.

Om nuläget består är informationsinhämtning möjlig endast om den är brottsrelaterad och sker innanför Finlands gränser, eller med sådana metoder för underrättelseinhämtning som inte anses förutsätta en särskild rättsgrund.

3.2.2 Förslag av arbetsgruppen för en informationsanskaffningslag

Arbetsgruppen för en informationsanskaffningslag föreslog i sitt betänkande att det för de militära och civila myndigheter som svarar för den nationella säkerheten ska föreskrivas om befogenheter till personbaserad underrättelseinhämtning som avser utländska förhållanden (i betänkandet ”personbaserad underrättelseinhämtning utomlands”), underrättelseinhämtning som avser utländska datasystem (i betänkandet ”spaning i utländska datasystem”) och underrättelseinhämtning som avser gränsöverskridande datatrafik (i betänkandet ”datatrafikspaning”). Med den civila myndighet som svarar för den nationella säkerheten avsåg arbetsgruppen skyddspolisen.

Med personbaserad underrättelseinhämtning som avser utländska förhållanden avsågs i arbetsgruppens betänkande underrättelseinhämtning som avser utländska förhållanden och sker genom personkontakt eller genom personligt iakttagande av en person eller ett annat objekt. Med underrättelseinhämtning som avser utländska datasystem avsågs i betänkandet spaning som görs med datatekniska metoder och som inriktas på uppgifter som behandlas i datasystem utomlands. Med underrättelseinhämtning som avser datatrafik avsåg arbetsgruppen spaning som inriktar sig på den datatrafik som rör sig i de datakommunikationstrådar som överskrider den finska gränsen.

De av arbetsgruppen föreslagna metoderna underrättelseinhämtning som avser utländska datasystem och personbaserad underrättelseinhämtning som avser utländska förhållanden handlar om verksamhet som äger rum utomlands (underrättelseinhämtning som avser utländska förhållanden).

Syftet med både underrättelseinhämtning som avser datatrafik och underrättelseinhämtning som avser utländska förhållanden är enligt arbetsgruppen att inhämta sådan underrättelseinformation om allvarliga internationella hot som är nödvändig med tanke på den nationella säkerheten. Genom verksamheten stöds den högsta statsledningens beslutsfattande, samtidigt som det säkerställs att beslutsfattandet bygger på korrekt, aktuell och tillförlitlig information. Genom verksamheten möjliggörs också att behöriga myndigheter vidtar åtgärder för att avvärja hoten.

Kontaktytan mellan underrättelseinhämtning och avvärjande åtgärder behöver organiseras särskilt. Utgående från den information som erhålls genom spaning måste den behöriga myndigheten kunna vidta nödvändiga åtgärder för att avvärja ett hot.

Underrättelseinhämtningen bör övervakas såväl juridiskt som parlamentariskt. Det är befogat att ordna övervakningen av de olika underrättelsemetoderna så enhetligt som möjligt.

Arbetsgruppen för en informationsanskaffningslag föreslog att de befogenheter som hör samman med civil underrättelseinhämtning ska beredas vid inrikesministeriet och att de befogenheter som hör samman med militär underrättelseinhämtning ska beredas vid försvarsministeriet. Eftersom underrättelseinhämtning som avser datatrafik behövs inom vartdera förvaltningsområdet bör det enligt arbetsgruppen övervägas om en särskild lag om underrättelseinhämtning som avser datatrafik ska stiftas.

Arbetsgruppen tog dock inte ställning till i vilka lagar som inrikesministeriet respektive försvarsministeriet har föredragningsansvaret för det bör föreskrivas om befogenheter, beslutsfattande och övervakningsmekanismer för underrättelseverksamhet, utan till denna del lämnades lagstiftningslösningen öppen.

3.2.3 Förslag av arbetsgruppen för en lag om militär underrättelseverksamhet

Det förslag som arbetsgruppen för en lag om militär underrättelseverksamhet gav baserade sig på det betänkande som arbetsgruppen för en informationsanskaffningslag hade gett. Därmed anammades största delen av de lösningar som arbetsgruppen för en informationsanskaffningslag hade gått in för också i det betänkande som arbetsgruppen för en lag om militär underrättelseverksamhet gav.

Arbetsgruppen för en lag om militär underrättelseverksamhet ansåg att det är motiverat att befogenheter till underrättelseinhämtning som avser utländska förhållanden, dvs. personbaserad underrättelseinhämtning och underrättelseinhämtning som avser datasystem, möjliggörs också inom Finland. Enligt arbetsgruppens uppfattning är syftet med befogenheterna till underrättelseinhämtning att avvärja hot mot landets försvar och den nationella säkerheten. Även om de allvarligaste faktorerna som hotar Finlands säkerhet numera ofta anknyter till händelser utanför Finland och det är lättare hänt än förr att följderna av hot som har utländskt ursprung eller uppkommer utomlands realiseras i Finland, går det ändå inte att med hjälp av befogenheter till underrättelseinhämtning som avser utländska förhållanden inhämta sådan information i Finland som är nödvändig för landets försvar och den nationella säkerheten.

Eftersom bestämmelserna om Försvarsmaktens brottsbekämpning inte finns i lagen om försvarsmakten utan i en separat lag gick arbetsgruppen in för att föreslå ett alternativ där det stiftas en ny lag om militär underrättelseverksamhet som innehåller bestämmelser om organiseringen och styrningen av samt tillsynen över den militära underrättelseverksamheten, om den militära underrättelseverksamhetens befogenheter och om den interna övervakningen.

*Organisering av den militära underrättelseinhämtningen*

Som framgår av den internationella jämförelsen kan underrättelseverksamheten organiseras på många olika sätt. I vissa stater, bland dem Schweiz och Tyskland, har man valt en lösning där underrättelseinhämtning som avser utländska förhållanden har avskilts från statens interna underrättelseinhämtning. I detta alternativ inhämtar underrättelsetjänsten för utlandet information på både den militära och den civila underrättelseinhämtningens område för den högsta statsledningens bruk, och statens interna underrättelseinhämtning inriktar sig framför allt på brottsbekämpning. I de länder som det hänvisas till här ovan är den centrala underrättelsetjänsten för utlandet en civil myndighet.

I den centraliserade modellen har styrningen av den underrättelseinhämtning som avser utländska förhållanden koncentrerats till förvaltningsområdet för den myndighet som sköter den underrättelseinhämtning som avser utländska förhållanden. Underrättelseverksamhet som avser utländska förhållanden kräver inte någon särskild samordning mellan olika underrättelsemyndigheter.

För att det ska gå att från den underrättelseinhämtning som avser utländska förhållanden lämna ut uppgifter för att användas inom den inre säkerheten, exempelvis för kriminalunderrättelseinhämtning och brottsbekämpning, krävs administrativa arrangemang eftersom underrättelseinhämtning som avser utländska förhållanden har en annan typ av uppdrag och finns inom ett annat förvaltningsområde.

I vissa stater, t.ex. Nederländerna, har man gått in för att skilja åt den militära underrättelseinhämtningen från den civila. När underrättelseverksamheten organiseras på det sättet får både den myndighet som bedriver underrättelseinhämtning i fråga om hot av civil karaktär och den militära underrättelseinhämtningsaktören inhämta information som anknyter till sina egna arbetsuppgifter.

Föremålen för underrättelseinhämtning kan vara åtminstone delvis överlappande inom den militära och den civila underrättelseinhämtningen. Utlämnandet av underrättelseuppgifter från underrättelseverksamheten till brottsbekämpning kan visserligen anses vara lättare, eftersom underrättelseinhämtningsaktörerna och de brottsbekämpande myndigheterna finns inom samma förvaltningsområde.

I Finland behöver inte nya myndigheter inrättas, om underrättelseinhämtningen decentraliseras så att den militära sidan hålls åtskils från den civila. Decentraliserad underrättelseinhämtning förutsätter emellertid mer omfattande styrning från den högsta statsledningens sida när föremålen för underrättelseinhämtning bestäms, och intensiv samordning av underrättelseverksamheten på operativ nivå behövs också.

*Personbaserad underrättelseinhämtning och teknisk informationsinhämtning*

Den personbaserade underrättelseinhämtningen kan delas upp i befogenheter som det redan föreskrivs om i 5 kap. i polislagen, där de benämns metoder för inhämtande av information. Den personbaserade underrättelseinhämtningen är uppdelad i teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, optisk observation, inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp, användning av informationskällor, platsspecifik underrättelseinhämtning och kopiering.

Dessutom är det ändamålsenligt att föreskriva om underrättelseinhämtning som avser utländska datasystem och om radiosignalspaning, vilka är tekniska metoder för informationsinhämtning. Teknisk observation av utrustning och underrättelseinhämtning som avser utländska datasystem är likartade metoder för inhämtning av information. Skillnaden mellan dem är emellertid att underrättelseinhämtning som avser utländska datasystem är långvarig och omfattande verksamhet som inte nödvändigtvis riktas mot en viss person. Bestämmelser om radiosignalspaning föreslås också, uttryckligen på grund av verksamhetens betydelse.

Det föreslås att befogenheterna ska utövas för inhämtande av information om verksamhet som är föremål för militär underrättelseinhämtning.

Att föreskriva om alla befogenheter i lagen om militär underrättelseverksamhet är ändamålsenligt med tanke på lagens systematik och överskådlighet.

*Underrättelseinhämtning som avser datatrafik*

Vid underrättelseinhämtning som avser datatrafik inhämtas information ur kommunikation som rör sig över Finlands gräns i datanät. I en del stater riktas underrättelseinhämtning som avser datatrafik i princip mot all kommunikation oberoende av var kommunikationen försiggår. För att underrättelseinhämtning som avser datatrafik ska kunna riktas mot all meddelandetrafik förutsätts synnerligen stora resurser för lagring, hantering och analysering av informationen. Dessutom kan underrättelseinhämtning som avser datatrafik och som riktas mot all datatrafik inte anses vara acceptabel med tanke på människorättskonventionen och människorättsdomstolens avgörandepraxis, även om den skulle kunna ge heltäckande information om hot mot den nationella säkerheten.

Vid riktad underrättelseinhämtning som avser datatrafik strävar man efter att inhämta information om ett visst objekt som är av betydelse för underrättelseinhämtningen. Ofta föregås inledandet av underrättelseinhämtning som avser datatrafik av att man redan på något annat sätt har fått information om ett behov av att rikta underrättelseinhämtning som avser datatrafik mot ett visst håll. Eftersom underrättelseinhämtning som avser datatrafik har kunnat riktas redan i förväg, kräver den inte lika stora resurser som icke riktad underrättelseinhämtning som avser datatrafik. I det riktade alternativet går man inte heller rakt på meddelandets innehåll, annat än i vissa fall som det föreskrivs om särskilt, t.ex. sabotageprogram och en främmande stats väpnade styrkors meddelandetrafik.

Det riktade alternativet kan också anses vara acceptabelt med tanke på människorättsdomstolens avgörandepraxis.

Ett alternativ i fråga om underrättelseinhämtning som avser datatrafik är en riktad modell av typ tvångsmedel, där underrättelsemyndigheten får den information som den behöver av en teleoperatör och inte i något som helst skede har teknisk åtkomst till den övriga meddelandetrafiken i datakommunikationstrådarna. I denna modell är teleoperatören den som genomför underrättelseinhämtningen tekniskt, och militärunderrättelsemyndigheten begär att få av teleoperatören den information som militärunderrättelsemyndigheten med stöd av ett domstolstillstånd har rätt att inhämta i datakommunikationsnätet. En lösning av typ tvångsmedel skulle kunna möjliggöras t.ex. genom att kriminalisera förehavanden som äventyrar stats- eller samhällsordningen, såvida de inte nu omfattas av strafflagen, och genom att utsträcka det materiella eller geografiska tillämpningsområdet för de tvångsmedel som Försvarsmakten har tillgång till. Med dessa metoder skulle det inte vara möjligt att inhämta information ur datatrafik som överskrider Finlands gräns.

Riktande av denna typ av underrättelseinhämtning som avser datatrafik förutsätter också att man har förhandskännedom om information som hänför sig till en teleadress eller teleterminalutrustning. Modellen förutsätter också att det föreskrivs om vidsträckta skyldigheter för teleoperatörerna, som är centrala datatrafikaktörer, att bevara och lämna ut uppgifter.

Ett annat alternativ är en modell där datatrafiken sållas automatiskt med hjälp av sökbegrepp. Med beaktande av informationsmängden i de datakommunikationstrådar som överskrider Finlands gränser skulle ett alternativ där enbart automatiska sökbegrepp används vara svårt att genomföra och ställa synnerligen stora resurskrav på verksamheten.

Underrättelseinhämtning som avser datatrafik kan genomföras också på så sätt att det tekniska genomförandet av den koncentreras till en enda myndighet eller decentraliseras till flera myndigheter. I den centraliserade modellen samlas de resurser som krävs för underrättelseinhämtning som avser datatrafik hos en enda aktör, varvid andra aktörer inte behöver utveckla och skaffa resurser för ändamålet. För andra myndigheter kan det föreskrivas om behörighet att ge uppdrag att inhämta information genom underrättelseinhämtning som avser datatrafik.

*Kopplingar som underrättelseinhämtning som avser datatrafik förutsätter*

Som man kan se av människorättsdomstolens ovan beskrivna avgörandepraxis kan underrättelsemyndigheten inte ha direkt och obegränsad åtkomst till datatrafiknäten. Detta krav kan uppfyllas genom att den koppling till datatrafiknätet som anges i det domstolstillstånd som underrättelseinhämtning som avser datatrafik förutsätter utförs av någon annan än underrättelsemyndigheten själv. I Finland kan Kommunikationsverket, en teleoperatör, Statens center för informations- och kommunikationsteknik Valtori eller det av staten helägda företaget Suomen turvallisuusverkko Oy vara sådana parter. Att utföra en koppling som överensstämmer med ett domstolstillstånd och att verkställa tillståndet till denna del kan inte anses vara betydande utövning av offentlig makt, därför skulle det kunna uppdras också åt andra än myndigheter. Utförandet av kopplingen är inte heller en fråga om övervakning utan om verkställighetsåtgärder.

Vad utförandet av kopplingar beträffar gäller det dessutom att beakta att när verksamheten utvecklas får den som utför kopplingar unika kunskaper om det finska kommunikationsnätet och datatrafiken i det. Det är inte ändamålsenligt att den som utför en koppling kan utnyttja dessa kunskaper i sin affärsverksamhet för att nå ett ekonomiskt resultat.

Kommunikationsverket svarar för sin del för att datanäten fungerar utan störningar och för att verksamhetsutövarna får den information om sabotageprogram i datanäten som behövs. Vidare har Kommunikationsverket tillräcklig kompetens och tillräckliga resurser för att underrättelsemyndigheten, efter att ha fått tillstånd av domstolen, ska kunna verkställa tillståndet så snabbt och ändamålsenligt som möjligt. När kopplingen utförs fullgör Kommunikationsverket för sin del också sin uppgift för att underrättelsemyndigheten inte ska ha obegränsad åtkomst till datatrafiknätet. Visserligen kan Kommunikationsverkets möjligheter att bedriva internationellt samarbete inom branschen bli lidande, om verket bistår underrättelsemyndigheten.

Ett annat alternativ är att kopplingen utförs av den teleoperatör som administrerar den kommunikationsnätsdel som den underrättelseinhämtning som avser datatrafik inriktas på. Teleoperatörerna har behövlig kompetens och resurser för att utföra kopplingen och behov av att utföra den så, att datatrafiken orsakas så liten olägenhet som möjligt. Den föreslagna lagen medför visserligen redan nu nya skyldigheter för teleoperatörer. Dessutom ger de nya uppgifterna upphov till direkta kostnader för teleoperatörerna, kostnader som underrättelsemyndigheten

föreslås vara skyldig att ersätta. Teleoperatörerna kan inte heller anses vara tillräckligt utomstående med tanke på underrättelseinhämtning som avser datatrafik. Att en teleoperatör fungerar som den som tekniskt genomför en koppling skulle likaså kunna vara problematiskt när man beaktar underrättelseverksamhetens känsliga natur och sekretessintresset.

Som ett tredje alternativ skulle man kunna överväga Valtori. Bestämmelser om Valtoris uppgifter och om de tjänster som Valtori tillhandahåller finns i lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013). Valtori tillhandahåller branschoberoende ICT-tjänster inom statsförvaltningen. Målet är att de branschoberoende ICT-tjänsterna ska vara konkurrenskraftiga, av hög kvalitet, ekologiska, informationssäkra och uppfylla kundernas behov. Inom Valtori finns en TUVE-avdelning, som ska tillhandahålla de statliga ämbetsverk och inrättningar som nämns i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) informations- och kommunikationstekniska tjänster samt integrationstjänster som uppfyller kraven på hög beredskap och hög säkerhet.

Ett fjärde alternativ är ett dotterbolag som Suomen Erillisverkot Oy heläger och som grundades med tanke på den offentliga förvaltningens säkerhetsnätsverksamhet, dvs. Suomen Turvallisuusverkko Oy. Enligt 6 § 1 mom. i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät är Suomen Erillisverkot Oy ett aktiebolag som helt och hållet ägs av staten. Enligt 2 mom. är dessutom syftet med bolagets verksamhet vid skötseln av de uppgifter som anges i lagen inte att uppnå företagsekonomisk vinst.

3.2.4 Bedömning av alternativen

I nuläget kan myndigheterna inhämta information endast på brottsrelaterade grunder. Brottsrelaterad informationsinhämtning är emellertid inte ett heltäckande svar på de frågor som man vill få besvarade genom underrättelseverksamhet.

Nykriminaliseringar och utvidgning av området för vissa kriminaliseringar kan inte heller anses vara en ändamålsenlig lösning från rättssystemets synpunkt, eftersom det har fastställts att kriminalisering alltid ska vara ett sistahandsalternativ i samhällsverksamheten. Dessutom skulle alternativet förutsätta att det föreskrivs om nya befogenheter som gäller den militära underrättelseinhämtningen.

När det gäller organisering av underrättelseverksamheten skulle en centraliserad modell med en underrättelsetjänst för utlandet kräva att en ny myndighet inrättas i Finland och att helt nya verksamhetssätt skapas inom myndigheten. Vidare skulle det bli nödvändigt att för statens interna informationsinhämtnings vidkommande överväga att vidareutveckla de behöriga myndigheternas befogenheter till informationsinhämtning.

Behoven inom försvarsministeriets förvaltningsområde gäller formande och upprätthållande av en lägesbild som hänför sig till Försvarsmaktens uppgifter, givande av förhandsvarning och målidentifieringsstöd. Detta förutsätter ingående förhandskännedom om verksamhetsfältet och objekten samt förhandskunskaper om verksamhetsfältets praxis och verksamhetssätt. Försvarsmakten har undersökt och följt dessa ända sedan den inrättades, vilket innebär att det är ändamålsenligast att den militära underrättelseverksamheten bedrivs inom försvarsförvaltningen. Behoven inom inrikesministeriets förvaltningsområde anknyter för sin del till upptäckande av allvarliga hot av civil karaktär som riktas mot den nationella säkerheten, t.ex. terrorism och spionage, och identifiering av bakgrundsaktörerna. Därför är det möjligt att bereda lagstiftningen om civil underrättelseinhämtning under inrikesministeriets ledning.

En av de viktigaste uppgifterna för den militära underrättelseinhämtningen är att så långt som möjligt producera realtidsinformation om säkerhetsmiljöns utveckling, vilket tangerar frågor kring t.ex. materiel som främmande staters väpnade styrkor skaffar och övningar som de planerar och genomför. För att nämna ett exempel anses just sedvanlig materielanskaffning till väpnade styrkor och sådana styrkors övningsverksamhet allmänt taget inte vara brottslig verksamhet, om den sker inom de gränser som tillåts i internationella avtal och i lagstiftningen, vilket innebär att det inte är en gångbar lösning att kriminalisera verksamheten på nationell lagstiftningsnivå. Därmed lämpar sig den ovan beskrivna lösningsmodellen av tvångsmedelstyp inte direkt för den militära underrättelseinhämtningens behov.

Den föreslagna modellen med decentraliserad underrättelseinhämtning förutsätter att underrättelseverksamheten styrs och att samordningen av den är intensiv, såväl inom statsförvaltningen som mellan de operativa aktörerna.

Det kan anses att underrättelseinhämtning som avser datatrafik utförs effektivast när den inriktas så noggrant som möjligt på parter och verksamhet som kan ge information som är så nyttig som möjligt med tanke på underrättelseinhämtningen.

Den militära underrättelseinhämtningen är verksamhet som går ut på att producera sådan underrättelseinformation om utländska aktörer och förhållanden som är nödvändig med tanke på landets försvar och den nationella säkerheten, för att syftet med Försvarsmaktens verksamhet ska fullgöras ändamålsenligt och den högsta statsledningens beslutsfattande stödjas. Ytterligare är avsikten att upptäcka och identifiera yttre hot och samla in sådan information om dem som gör det möjligt att forma en lägesbild, vidta åtgärder för avvärjande av hoten och, för de militära myndigheternas del, ge en förhandsvarning. Den militära underrättelseinhämtningen är inte på samma sätt kopplad till personer och brott som brottsförebyggandet. Underrättelseinhämtning som avser datatrafik syftar till att från den militära underrättelseinhämtningens synpunkt reda ut handlingssätt som är mer generella till sin art än gärningar som betraktas som brottslig verksamhet.

I Finland bedriver bara Försvarsmakten militär underrättelseinhämtning. Den militära underrättelseinhämtningen är en kritisk del av det militära försvaret, som i sin tur är en av Försvarsmaktens lagstadgade uppgifter. Försvarsmakten själv kan anses ha den bästa kunskapen om hurdan militär underrättelseinformation den behöver för att kunna sköta sina lagstadgade uppgifter och med vilka metoder informationen går att inhämta på lämpligt sätt. Det är alltså inte ändamålsenligt att någon annan myndighet skulle syssla med militär underrättelseinhämtning vid sidan av eller i stället för Försvarsmakten. Den militära underrättelseinhämtningen skiljer sig kraftigt från t.ex. civil underrättelseinhämtning, därför är det ändamålsenligt att bestämmelserna om militär underrättelseinhämtning samlas i en lag för sig.

Regeringens strategimöte 20.8.2015 stannade för en modell där lagstiftningen om civil underrättelseverksamhet bereds under ledning av inrikesministeriet och lagstiftningen om militär underrättelseverksamhet bereds under ledning av försvarsministeriet.

Det tekniska genomförandet av underrättelseinhämtning som avser datatrafik bör vara myndighetsverksamhet. I verksamheten är det nödvändigt att behandla sådan sekretessbelagd information som allvarligt skulle äventyra den nationella säkerheten om den läckte ut. Dessutom ingriper verksamheten i de grundläggande fri- och rättigheterna på ett sätt som inte kan anses vara acceptabelt med tanke på 124 § i grundlagen. Av den anledningen är underrättelseinhämtning som avser datatrafik inte möjlig att utföra med hemliga metoder för inhämtande av

information och hemliga tvångsmedel, eftersom arrangemanget skulle förutsätta att utövning av offentlig makt överförs i betydande utsträckning till privata aktörer, teleoperatörer.

Från resurssynpunkt är det ändamålsenligast att det tekniska genomförandet av underrättelseinhämtning som avser datatrafik koncentreras till en enda myndighet. På så sätt utvecklar inte flera olika aktörer egna tekniska lösningar. Detta kan också anses förbättra uppföljningen av de resurser som anvisas för det tekniska genomförandet. Inte heller åläggs privata aktörer stora skyldigheter.

Ändamålsenligast är det att till myndighet med ansvar för underrättelseinhämtning som avser datatrafik utse en myndighet som redan har den tekniska kompetens och de internationella samarbetskontakter som underrättelseinhämtningen förutsätter. Cybersäkerhetscentret, som är med om att avvärja hot från internet, har den tekniska kompetens som verksamheten förutsätter. Centret har emellertid inte uppgifter som anknyter till inhämtningen av underrättelseuppgifter, och därmed inte heller sådana samarbetskontakter som underrättelseverksamheten förutsätter. Centralkriminalpolisen å sin sida har internationella samarbetskontakter. Den svarar dock för att brott som hör till dess verksamhetsområde reds ut och ser till att teletvångsmedel som hänför sig till polislagen och tvångsmedelslagen genomförs tekniskt med tanke på den straffrättsliga processen. Inte heller är centralkriminalpolisen nu på väg att få befogenheter till underrättelseinhämtning som avser datatrafik, utan för den civila underrättelseinhämtningens del föreslås skyddspolisen utöva befogenheter till underrättelseinhämtning som avser datatrafik. Skyddspolisen bedriver internationellt samarbete i samband med inhämtningen av underrättelseuppgifter, men har inte de resurser som det tekniska genomförandet av underrättelseinhämtning som avser datatrafik kräver. Försvarsmaktens underrättelsetjänst för sin del har både den tekniska kompetens som verksamheten förutsätter och sådana internationella samarbetskontakter som underrättelseverksamheten förutsätter. Med hänsyn till de ovannämnda omständigheterna kan Försvarsmaktens underrättelsetjänst anses vara det ändamålsenligaste alternativet som teknisk genomförare av underrättelseinhämtning som avser datatrafik.

I den centraliserade lösningen anvisas det tekniska genomförandet av underrättelseinhämtning som avser datatrafik militärunderrättelsemyndigheten (Huvudstabens underrättelseavdelning och Försvarsmaktens underrättelsetjänst), som på uppdrag av den uppdragsgivande myndigheten, dvs. skyddspolisen, sköter det tekniska genomförandet av underrättelseinhämtning som avser datatrafik.

För en centraliserad lösning talar kraven på att verksamheten är enhetlig och hemlighålls, den specialisering och tekniska kompetens som verksamheten förutsätter, kostnaderna för verksamheten och synpunkterna på övervakning av verksamhetens lagenlighet. Människorättsdomstolen har förutsatt att tydliga förfaranden skapas för underrättelseinhämtning som avser datatrafik och att verksamheten omfattas av laglighetsövervakning. Dessa omständigheter är lättast att tillgodose i den centraliserade modellen. Aspekter som rör enhetliga förfaranden och laglighetsövervakningen talar likaså för att det tekniska genomförandet av den militära underrättelseinhämtningen koncentreras till en enda myndighet. Även ekonomiska orsaker talar för alternativet. Försvarsmaktens underrättelsetjänst har redan för närvarande både de tekniska förutsättningarna för verksamheten och de internationella samarbetskontakter som behövs.

Organiseringen av underrättelseinhämtning som avser datatrafik förutsätter att teleföretag eller den som administrerar en gränsöverskridande kommunikationsnätsdel åläggs en skyldighet att bistå vid byggandet av en accesspunkt och att lämna de uppgifter som byggandet förutsätter till den part som svarar för att underrättelseinhämtning som avser datatrafik genomförs. Genomförandet får inte leda till att den allmänna datatrafiken blir långsammare. Anslutningen

bör planeras i samarbete med de parter som äger eller administrerar kommunikationsnät så, att olägenheterna för dem och för kommunikationsnätens funktion minimeras. Utgångspunkten är att direkta kostnader som den tekniska verksamheten eventuellt föranleder företagen ska täckas av de parter som använder underrättelseinhämtning som avser datatrafik.

Underrättelseverksamhet som riktas mot förtrolig kommunikation kan i nuläget anses vara möjlig endast i situationer där den part som är föremål för underrättelseinhämtning inte åtnjuter skydd för de grundläggande fri- och rättigheterna. Av denna orsak är en ändring av 10 § i grundlagen en förutsättning för den i denna proposition beskrivna underrättelseinhämtningen som avser datatrafik och i fråga om andra befogenheter när de ingriper i skyddet för förtroliga meddelanden.

Underrättelseinhämtning som riktar sig mot förtrolig kommunikation bör vara så riktad och avgränsad som möjligt. Föremålen för underrättelseinhämtning som avser datatrafik får inte vara slumpmässigt valda. Den myndighet som utför underrättelseinhämtning som avser datatrafik bör därmed ha en uppfattning om vilken kommunikation den underrättelseinhämtning som avser datatrafik ska riktas mot vid respektive tillfälle. För att nämna ett exempel skulle underrättelseinhämtning som avser datatrafik och riktas mot kommunikationen mellan en främmande stats myndigheter vara ändamålsenligt riktad och lättare att genomföra. När underrättelseinhämtning som avser datatrafik inriktas på andra aktörer förutsätts det att sökkategorier och automatiska sökbegrepp används, och i och med detta kan underrättelseinhämtning som avser datatrafik inriktas så effektivt som möjligt på det önskade objektet, varvid det kan anses att den är adekvat riktad.

Riktad underrättelseinhämtning som avser datatrafik kräver inte lika stor kapacitet att lagra och analysera information som icke riktad underrättelseinhämtning som avser datatrafik. Dessutom kan det anses att inverkan på t.ex. teleoperatörerna blir mindre.

Den koppling som underrättelseinhämtning som avser datatrafik förutsätter skulle kunna utföras av ett dotterbolag som Suomen Erillisverkot Oy heläger, dvs. Suomen Turvallisuusverkko Oy. För lösningen talar att dotterbolaget enligt vad som föreskrivs i lag ägs av Suomen Erillisverkot Oy, som är i statens ägo. Dessutom har Suomen Turvallisuusverkko Oy den kompetens som kopplingsarbetet förutsätter.

Ytterligare stöd får lösningen av konkurrensrättsliga aspekter. Om uppdraget gavs till en privat teleoperatör skulle denna med stöd av lag få sådana unika kunskaper om kommunikationsnäten i Finland som konkurrenterna inte skulle få. Genomförandet av kopplingen förutsätter också samverkan med alla teleoperatörer, därför kan det inte anses vara ändamålsenligt att den som utför kopplingen har möjlighet att med stöd av lag få information om sina konkurrenter.

För att en lägesbild ska kunna formas behöver den högsta statsledningen i Finland information som produceras utgående från uppgifter som samlas in genom underrättelseinhämtning som avser datatrafik. Därför bör också den högsta statsledningen kunna framställa sådana begäranden om information som kan komma att tillgodoses med hjälp av underrättelseinhämtning som avser datatrafik. Begärandena om information bör emellertid kanaliseras via Försvarsmakten eller skyddspolisen till den som tekniskt genomför underrättelseinhämtning som avser datatrafik. På så sätt kan den myndighet som fått en begäran om information överväga i varje enskilt fall vilken metod för underrättelseinhämtning som är ändamålsenligast för inhämtande av de uppgifter som avses i begäran om information.

### 3.3 De viktigaste förslagen

Regeringens proposition har utarbetats med utgångspunkt i arbetsgruppsbetänkandet ”Riktlinjer för en finsk underrättelselagstiftning” och skrivningar i statsminister Juha Sipiläs strategiska regeringsprogram. Syftet med lagstiftningsarbetet är att skapa ett konsekvent och aktuellt regelverk om militär underrättelseinhämtning, som till alla delar motsvarar de krav som grundlagen ställer. I propositionen föreslås helt nya bestämmelser om militär underrättelseinhämtning. För närvarande finns det ingen reglering på lagnivå inom området.

I propositionen har de internationella avtal som gäller Ålands ställning och lagstiftningen om Ålands självstyrelse beaktats. Propositionen bedöms inte stå i strid med gällande reglering om Ålands särställning.

*Lagen om militär underrättelseverksamhet*

*Allmänna bestämmelser (1 kap.)*

Lagen föreslås bli tillämpad på Försvarsmaktens underrättelseverksamhet, dvs. militär underrättelseinhämtning, genom vilken information som anknyter till vissa av Försvarsmaktens uppgifter som anges i lagen om försvarsmakten inhämtas i förväg, undersöks och utnyttjas till stöd för den finska utrikes-, säkerhets- och försvarspolitiken och för kartläggning av yttre hot mot Finland. För att dessa uppgifter ska fullgöras är det meningen att information ur offentliga och icke-offentliga informationskällor ska kunna inhämtas genom militär underrättelseinhämtning.

I 2 § föreskrivs det om lagens förhållande till annan lagstiftning, framför allt Försvarsmaktens brottsbekämpning och civil underrättelseinhämtning som skyddspolisen utför. Det föreslås att bestämmelser om extern laglighetsövervakning av underrättelseverksamheten tas in i en separat lag. Det är meningen att en lag om behandling av personuppgifter inom Försvarsmakten ska innehålla bestämmelser om behandlingen av personuppgifter. I 3 § föreslås bestämmelser om syftet med den militära underrättelseinhämtningen.

I 4 § finns en uttömmande uppräkning av föremålen för militärunderrättelsemyndighetens informationsinhämtning. Inom den militära underrättelseinhämtningen får det enligt paragrafen inhämtas information om verksamhet, om den till sin art är militär. Detta omspänner 1) verksamhet som bedrivs av en främmande stats väpnade styrkor och av med dem jämförbara organiserade trupper samt förberedelse för sådan verksamhet, 2) underrättelseverksamhet som riktar sig mot Finlands försvar, 3) planering, tillverkning, spridning och användning av massförstörelsevapen, 4) en främmande stats utvecklande och spridning av militärmateriel, 5) en kris som hotar internationell fred och säkerhet, 6) verksamhet som hotar säkerheten vid internationella krishanteringsinsatser samt 7) verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och i samband med annan internationell verksamhet. I paragrafen föreskrivs det också om inhämtning av information om verksamhet som hotar den nationella säkerheten. Med det avses verksamhet som kan äventyra det finska försvaret eller som äventyrar samhällets vitala funktioner.

I kapitlet föreskrivs också om de allmänna principer som ska iakttas vid militär underrättelseinhämtning och om de myndigheter som utför militär underrättelseinhämtning. Militärunderrättelsemyndigheter är enligt förslaget Försvarsmaktens Huvudstab och Försvarsmaktens underrättelsetjänst. Förbudet mot diskriminering (8 §) är en bestämmelse av ny typ i befogenhetslagstiftningen; den kan anses vara ändamålsenlig på grund av underrättelseverksamhetens art och styra verksamheten så att denna riktas tillräckligt exakt.

De allmänna förutsättningarna för användning av metoder för underrättelseinhämtning (11 §) motsvarar de allmänna förutsättningar för hemliga metoder för inhämtande av information som det föreskrivs om i 5 kap. i polislagen. De särskilda förutsättningarna för användningen av metoder för underrättelseinhämtning är nivåindelade på motsvarande sätt som i 5 kap. i polislagen, men bestämmelserna om dem är inte samlade i en viss paragraf utan har placerats i befogenhetsbestämmelserna.

*Styrning av och tillsyn över den militära underrättelseinhämtningen (2 kap.)*

Enligt förslaget behandlar utrikes- och säkerhetspolitiska ministerutskottets sammanträde med republikens president i förberedande syfte de årliga prioriteringarna för den militära underrättelseinhämtningen (12 §). Redan för närvarande behandlar utrikes- och säkerhetspolitiska ministerutskottet förberedelsevis viktiga ärenden som gäller utrikes- och säkerhetspolitiken och viktiga ärenden av annat slag vilka gäller Finlands relationer till främmande makter, viktiga ärenden gällande den inre säkerheten i anslutning därtill samt viktiga ärenden som gäller totalförsvaret. De förberedelsevis behandlade prioriteringarna ska försvarsministeriet enligt förslaget ge till Försvarsmakten.

I propositionen föreslås det (13 §) att sådana begäranden om information som är förenliga med de ovannämnda prioriteringarna ska kunna framställas till Huvudstaben av republikens president, statsrådets kansli, utrikesministeriet och försvarsministeriet. Huvudstabens underrättelsechef föreslås fatta beslut om genomförande av den informationsinhämtning som begäran om information innebär och om givande av underrättelseuppdrag åt militärunderrättelsemyndigheten.

Eftersom underrättelseverksamheten är av vidsträckt betydelse i samhället bör den kunna samordnas mellan de myndigheter som är centrala (14 §). Vidare beaktas i paragrafen sådana situationer som kräver utrikespolitiskt övervägande.

Det är meningen att utrikes- och säkerhetspolitiska ministerutskottets sammanträde med republikens president ska ha tillsyn över att underrättelseverksamheten är förenlig med prioriteringarna (15 §). Försvarsministeriet ska ge en redogörelse åtminstone en gång per år, på begäran eller på eget initiativ. Vidare ska Huvudstaben ge försvarsministeriet en redogörelse för den militära underrättelseverksamheten, dess art och omfattning samt hur den har riktats.

*Samverkan med andra myndigheter och internationellt samarbete (3 kap.)*

För att underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt bör civilunderrättelsemyndigheten och militärunderrättelsemyndigheten samarbeta.

Vid behov ska militärunderrättelsemyndigheten samarbeta också med andra myndigheter och sammanslutningar (17 §). Hjälp som andra myndigheter ger kan behövas för att ett underrättelseuppdrag ska kunna genomföras på det taktiska planet. Vidare kan enligt förslaget uppgifter lämnas ut till sammanslutningar som har en viktig roll i Finlands totalförsvar.

Eftersom det i Finland finns flera myndigheter som bedriver informationsinhämtning i hemlighet kan t.o.m. stora arbetssäkerhetsrisker komma att förekomma vid den minitära underrättelseinhämtningen (18 §). Det kan tänkas att arbetssäkerhetsrisker uppträder framför allt i situationer där olika myndigheter i hemlighet opererar inom ett och samma område utan vetskap om varandra.

När det är förenligt med Finlands nationella intressen kan militärunderrättelsemyndigheten enligt förslaget, i anknytning till sina uppgifter eller för att skydda den nationella säkerheten, bedriva internationellt samarbete, dvs. byta underrättelseuppgifter med utländska underrättelse- och säkerhetstjänster och delta i internationellt samarbete med anknytning till inhämtandet och bedömningen av underrättelseuppgifter.

*Metoder för underrättelseinhämtning (4 kap.)*

I 4 kap. regleras militärunderrättelsemyndigheternas befogenheter. De befogenheter som det föreskrivs om i kapitlet motsvarar som metoder betraktat i huvudsak de hemliga metoder för inhämtande av information som i huvudsak anges i 5 kap. i polislagen. Dessutom är förutsättningarna för att använda metoder för underrättelseinhämtning motsvarande som i polislagen.

Med stöd av hänvisningar till polislagen som skrivits in i lagen om militär disciplin och brottsbekämpning inom försvarsmakten har Försvarsmakten tillgång till brottsrelaterade hemliga metoder för inhämtande av information. De föreslagna nya befogenheterna kan anses vara befogade därför att endast Försvarsmakten kan anses ha tillräcklig know-how i fråga om det militära verksamhetsfältet och hot mot landets försvar, samt kännedom om vad som är brukligt och praxis inom verksamhetsfältet. För att underrättelseverksamheten ska kunna genomföras på lämpligt sätt krävs bakgrundskunskaper av det slaget, så att militärunderrättelsemyndigheten får chansen att utnyttja information som är allra mest kritisk med tanke på landets försvar.

Beslutsfattandet om användningen av metoder för underrättelseinhämtning föreslås vara nivåindelat på motsvarande sätt som i 5 kap. i polislagen. För att nämna ett exempel fattar domstolen på yrkande av Huvudstabens underrättelsechef beslut om teleavlyssning och annan motsvarande informationsinhämtning, medan beslut om systematisk observation kan fattas av en för uppdraget förordnad militärjurist eller annan tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning. Det är i vissa situationer ändamålsenligt med bestämmelser om förfarandet i brådskande fall.

Giltighetstiden för tillstånd att använda metoder för underrättelseinhämtning föreslås vara högst sex månader. Detta innebär ändå inte automatiskt att tillstånd alltid kan sökas eller beslut alltid kan fattas för sex månader eller att tillstånd alltid bör beviljas för sex månader. Prövning som utgår från proportionalitetsprincipen och principen om minsta olägenhet förutsätts genom att uttrycket ”för högst sex månader åt gången” ingår i bestämmelserna.

Ett särskilt krav i samband med användning av metoder för underrättelseinhämtning är att yrkandet och beslutet ska innehålla en redogörelse för fakta. Militärunderrättelsemyndigheten åläggs att presentera och motivera de fakta på basis av vilka beslutsfattaren, t.ex. domstolen, kan dra sina egna slutsatser om huruvida det finns allmänna och särskilda förutsättningar att använda en metod för underrättelseinhämtning. Dessutom ska yrkandet och beslutet innehålla tillräckliga fakta om underrättelseuppdraget och om det i 4 § avsedda föremålet för militär underrättelseinhämtning.

Vissa metoder för underrättelseinhämtning kan inriktas också på en grupp av personer. Vid militär underrättelseinhämtning kan det framkomma behov av att följa en viss persongrupps verksamhet, och då gäller behovet av informationsinhämtning t.ex. hur gruppen är organiserad, personerna i gruppen och gruppens aktivitet inom ett visst område.

Förtäckt inhämtande av information (22–23 §) kan på motsvarande sätt riktas mot personer eller persongrupper. Alldeles som när det gäller andra metoder för underrättelseinhämtning ska också beslut om förtäckt inhämtande av information innehålla de fakta som inhämtandet av information grundar sig på och på basis av vilka en utomstående betraktare, t.ex. underrättelseombudsmannen som utför övervakning, kan dra sina egna slutsatser om förekomsten av förutsättningar för att använda metoden för underrättelseinhämtning. I paragrafen om beslut om förtäckt inhämtande av information finns en bestämmelse om beslutsförfarandet i brådskande situationer. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter att åtgärden har vidtagits.

Teknisk observation delas in i teknisk avlyssning (24–25 §), optisk observation (26–27 §), teknisk spårning (även teknisk spårning av en person) (28–29 §) och teknisk observation av utrustning (30–31 §). Den tekniska observation av utrustning som föreslås i propositionen avviker från definitionen av teknisk observation i 5 kap. i gällande polislag.

Vid militär underrättelseverksamhet kan teknisk observation av utrustning inriktas också på meddelandets innehåll, enligt förslaget. Att ta reda på innehållet i meddelanden som lagrats i en teknisk anordning, t.ex. en pekplatta, förefaller inte vara möjligt inom ramen för andra befogenheter. Teknisk avlyssning sker i det skede då ett meddelande skrivs, och teleavlyssning inriktas på meddelanden som är under förmedling i ett allmänt kommunikationsnät. Kriterierna för beslutsfattande föreslås vara desamma som när det gäller teleavlyssning.

I fråga om teleavlyssning och annat motsvarande inhämtande av information föreslås det att dessa metoder ska kunna riktas också mot personer vid sidan av teleadresser och teleterminalutrustning. När ett tillstånd till teleavlyssning avser en person är det meningen att tillståndet ska inbegripa de teleadresser eller teleterminalutrustningar som den person som anges i tillståndet till teleavlyssning innehar eller annars antas använda i övrigt. Ett tillstånd till teleavlyssning gäller alltså inte en specifik teleadress eller teleterminalutrustning.

I definitionen av begreppet teleavlyssning föreslås ett tillägg som gäller också andra kommunikationsförbindelser än ett allmänt kommunikationsnät. Det kan inte anses att definitionen av begreppet allmänt kommunikationsnät på ett tillräckligt sätt täcker de kommunikationsmedel som aktörer som är föremål för militär underrättelseverksamhet använder, t.ex. satellittelefoner. Andra befogenheter kan inte heller anses möjliggöra att underrättelseinhämtningen inriktas på meddelanden som redan har avgått från en satellittelefon. Exempelvis teknisk avlyssning inriktas på det skede då meddelandet ännu inte har skickats iväg.

Dessutom föreslås det bli möjligt att inrikta teleavlyssning på statliga aktörer under andra förutsättningar än på andra aktörer.

I kapitlet finns också bestämmelser om teleövervakning och sådan teleövervakning som sker med en persons samtycke (35–36 §). På motsvarande sätt som i fråga om teleavlyssning föreslås förutsättningarna för att inrikta teleövervakning på föremålet för ett underrättelseuppdrag skilja sig åt beroende på om det är fråga om en statlig eller en icke-statlig aktör.

Bestämmelser om inhämtande av basstationsuppgifter finns i 37–38 §.

I kapitlet finns också bestämmelser om inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning (39 §). I paragrafen föreskrivs det med avvikelse från 5 kap. i polislagen att en anordning för inhämtande av identifieringsuppgifter ska kunna användas också

för annat än för inhämtande av identifieringsuppgifter. Kommunikationsverket ska kontrollera anordningen.

I paragrafen om installation och avinstallation av anordningar, metoder eller programvara (40 §) föreskrivs det om en tjänsteman som är anställd vid militärunderrättelsemyndigheten och har rätt att vidta åtgärden. På så sätt utnyttjas bästa möjliga tekniska kompetens, vilket krävs när det gäller att installera och avinstallera anordningar, metoder eller programvara.

I 41–43 § föreskrivs det om täckoperationer, och bestämmelser om bevisprovokation genom köp finns i 45–48 §. Också brottsförbud har en väsentlig anknytning till täckoperationer (44 §).

Lagen föreslås också uppta bestämmelser om användning av informationskällor (49–51 §). I anknytning till detta föreslås det bli separat föreskrivet om tryggande av informationskällor (75 §). Tryggandet av informationskällor handlar om att skydda informationskällorna föregripande och mer intensivt än vad som möjliggörs i gällande lagstiftning om skyddande av verksamheten.

Begreppet platsspecifik underrättelseinhämtning definieras i 52 §. Med platsspecifik underrättelseinhämtning avses underrättelseinhämtning som ska företas på en plats som anges i paragrafen, för att påträffa ett föremål, egendom, dokument, information eller en omständighet. Platsspecifik underrättelseinhämtning får inte företas i ett utrymme som används för boende av permanent natur.

I 53 § föreskrivs det om beslut om platsspecifik underrättelseinhämtning. Frågan om vem som är behörig att fatta beslut är enligt paragrafen beroende av huruvida den platsspecifika underrättelseinhämtningen riktas mot en plats som man inte har allmänt tillträde till eller till vilken det allmänna tillträdet har begränsats eller förhindrats under den tidpunkt då den platsspecifika underrättelseinhämtningen genomförs. Om så är fallet beslutar domstolen om den platsspecifika underrättelseinhämtningen på yrkande av en militärjurist eller annan tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning. I annat fall beslutar Huvudstabens underrättelsechef eller en militärjurist eller annan tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning om den platsspecifika underrättelseinhämtningen.

I 54 § föreskrivs det om kopiering, som i likhet med platsspecifik underrättelseinhämtning är en ny metod för informationsinhämtning. Enligt paragrafen ska militärunderrättelsemyndigheten ha rätt att kopiera ett dokument eller ett annat föremål för att utföra ett underrättelseuppdrag.

I 55 och 56 § finns bestämmelser om kopiering av försändelser och kvarhållande av försändelser för kopiering. Det är fråga om metoder som motsvarar dem som det föreskrivs om i 7 kap. i tvångsmedelslagen. Vad användningsgrunderna och användningsändamålet beträffar är det i detta sammanhang fråga om metoder för underrättelseinhämtning. I 57 § finns bestämmelser om beslut om kopiering.

I 58–59 § föreskrivs det om radiosignalspaning. I sin nuvarande form kräver befogenheten ingen särskild reglering. Med tanke på den militära underrättelseverksamheten som helhet och metodens betydelse är det emellertid ändamålsenligt med en uttrycklig bestämmelse om befogenheten.

Bestämmelserna i 60–61 § gäller underrättelseinhämtning som avser utländska datasystem. Befogenheten kan anses vara delvis jämförbar med teknisk observation av utrustning och teknisk avlyssning, vilka metoder är i bruk i Finland. Eftersom användningen av underrättelseinhämtning som avser utländska datasystem ofta kan vara långvarig och långsiktig och eftersom utrikespolitiska aspekter som det gäller att överväga noggrant ofta hänför sig till den är det ändamålsenligt att föreskriva om befogenheten och om beslutsfattandet med anknytning till den som en separat befogenhet.

I 62 § föreskrivs det om militär underrättelseinhämtning utomlands. För att det ska vara möjligt att framgångsrikt trygga samhället behöver säkerhetsmyndigheterna i Finland kunna inhämta information också av och om utländska aktörer. Med underrättelseinhämtning som avser utländska förhållanden avses att information som är väsentlig med tanke på den nationella säkerheten och gäller utländska förhållanden och objekt inhämtas. Syftet med underrättelseinhämtning som avser utländska förhållanden är att samla in information som är nödvändig för den högsta statsledningens säkerhetspolitiska beslutsfattande och för avvärjningen av allvarliga yttre säkerhetshot. Alla metoder för underrättelseinhämtning avses kunna bli använda när det gäller militär underrättelseinhämtning utomlands. Vad beträffar innehållet i beslut, framställning och plan ska enligt förslaget iakttas det som föreskrivs i paragraferna om beslut om metoderna för underrättelseinhämtning. Vid underrättelseinhämtning som avser utländska förhållanden ska man därför ange samma saker i beslutet om metoden för underrättelseinhämtning som vid underrättelseinhämtning inom landet. Vissa lagbestämmelser avses emellertid inte bli tillämpade vid underrättelseinhämtning som avser utländska förhållanden.

Det är meningen att Huvudstabens underrättelsechef alltid ska besluta om militär underrättelseinhämtning utomlands och om den metod som ska användas. Detta är befogat på grund av de sensitiva utrikespolitiska element som är förknippade med underrättelseinhämtning som avser utländska förhållanden. De utrikespolitiska dimensioner som hör ihop med underrättelseinhämtning som avser utländska förhållanden avses också bli behandlade när den militära och den civila underrättelseinhämtningen samordnas, varvid de viktigaste utrikespolitiska parterna medverkar.

Separata bestämmelser om internationellt samarbete föreslås. Också härvid ska besluten om vilka metoder för underrättelseinhämtning som ska användas vid operationer som utförs utomlands fattas av Huvudstabens underrättelsechef. Skillnaden mellan internationellt samarbete och underrättelseinhämtning som avser utländska förhållanden ligger i huruvida den stat som är föremål för operationen är medveten om den eller inte. I princip utförs underrättelseinhämtning som avser utländska förhållanden utan att målstaten eller en tredje stat har kännedom om den, medan internationellt samarbete bedrivs utgående från målstatens samtycke, alternativt tillsammans med en tredje stat utan att målstaten har kännedom om saken.

*Informationsinhämtning som riktas mot datatrafik*

I lagen föreslås bestämmelser om befogenheter till underrättelseinhämtning som riktas mot datatrafik.

Med underrättelseinhämtning som avser datatrafik avses teknisk informationsinhämtning riktad mot datatrafik som rör sig i en del av ett kommunikationsnät som överskrider Finlands gräns, vilken baserar sig på automatiserad avskiljning av datatrafiken samt behandling av den inhämtade informationen. Underrättelseinhämtning som avser datatrafik riktas därmed endast mot datatrafik som överskrider riksgränsen genom att övergå från ett finskt kommunikations-

nät till ett utländskt eller vice versa. En stor del av den finska datatrafiken utesluts redan på så sätt ur underrättelseinhämtning som avser datatrafik.

En allmän förutsättning också för underrättelseinhämtning som riktas mot datatrafik är att verksamheten är resultatrik särskilt när underrättelseinhämtning som avser datatrafik kan riktas enbart mot en statlig aktörs datatrafik (65 §). Förutsättningen kan anses vara tillräcklig, eftersom stater och parter som kan jämställas med dem inte åtnjuter skydd för hemligheten för förtrolig kommunikation.

I andra fall är det, utöver kravet på resultatrikedom, en förutsättning för underrättelseinhämtning som avser datatrafik att den är nödvändig, vilket är den högsta förutsättningströskel som lagstiftningen om myndigheternas befogenheter känner till (67 §). Nödvändighetsförutsättningen avses bli tillämpad både i sådana fall där föremålet i sig för underrättelseinhämtning som avser datatrafik är en främmande stat men sökbegrepp kan komma att användas också i fråga om annan datatrafik, och i sådana fall där föremålet för underrättelseinhämtning som avser datatrafik åtnjuter direkt skydd för hemligheten för förtroliga meddelanden.

Nödvändighetsförutsättningen innebär att metoden ska tillgripas som sista alternativ, dvs. i en situation där det är omöjligt eller orimligt svårt att inhämta informationen på något annat sätt. För att förutsättningen ska tillämpas krävs det att både Försvarsmaktens underrättelsetjänst, som söker tillstånd till underrättelseinhämtning som avser datatrafik, och den domstol som avgör tillståndsyrkandet gör en jämförelse mellan de befogenheter som det föreskrivs om i 4 kap. och underrättelseinhämtning som avser datatrafik. Om det inte är omöjligt eller orimligt svårt att använda andra metoder för underrättelseinhämtning, ska de användas i första hand.

Definitionen av begreppet kommunikationsnät är teknikneutral. Eftersom största delen av datatrafiken mellan Finland och utlandet förmedlas via optisk fiber i dataöverföringskablar riktas underrättelseinhämtning som avser datatrafik i praktiken huvudsakligen mot trådbunden datatrafik. Tack vare att begreppet kommunikationsnät är teknikneutralt säkerställs det emellertid att lagen är tillämplig också i andra tekniska miljöer och vid förändringar i kommunikationstekniken.

I kapitlet föreskrivs det också om insamling och behandling av tekniska data som är nödvändig för att inrikta informationsinhämtning som avser datatrafik i ett kommunikationsnät (63 §). Analys av dessa data är en nödvändig förutsättning för att det ska gå att så noggrant som möjligt inrikta underrättelseinhämtning som avser datatrafik på en viss kommunikationsnätsdel som överskrider Finlands gräns. Det som analyseras är datatrafikflödena. Dessutom föreskrivs det (95 §) att ägare och innehavare av kommunikationsnät ska vara skyldiga att bistå genom att ge Försvarsmaktens underrättelsetjänst de tekniska data som de förfogar över och som behövs för att kommunikationsnätsdelen ska kunna specificeras.

Underrättelseinhämtning som avser datatrafik bygger som metod på automatiserad avskiljning av datatrafiken. Detta skiljer den från de andra metoder för underrättelseinhämtning som riktas mot elektronisk kommunikation, t.ex. teleavlyssning och teleövervakning. Det är inte fråga om informationsinhämtning som riktas mot en enskild känd teleadress eller teleterminalutrustning, utan om filtrering av datatrafiken med automatiska metoder vid en sådan punkt i ett kommunikationsnät via vilken den datatrafik som är föremål för underrättelseinhämtningen kan antas gå. En lösning som baserar sig på att datatrafiken filtreras möjliggör att kommunikation som anknyter till hot upptäcks och att bakgrundskrafterna identifieras och lokaliseras. Filtreringen är tänkt att skötas så, att det datatrafikflöde som valts ut jämförs mot sökbegrepp,

dvs. kriterier som ställts upp i förväg. Datatrafikflödet jämförs alltså mot sökbegrepp och kategorier av sökbegrepp.

Som sökbegrepp är det enligt förslaget tillåtet att använda andra uppgifter än sådana som beskriver ett förtroligt meddelandes semantiska innehåll, framför allt uppgifter som gäller styrning och förmedling av datatrafiken, dvs. sådana instruktioner, kommandon och andra metadata som är avsedda för datanätet eller för det avsändande eller mottagande datasystemet och med vars hjälp transporten och styrningen av meddelandet i kommunikationsnätet och datasystemet påverkas. Som sökbegrepp tillåts också t.ex. uppgifter om användningen av något krypteringsprogram.

Ett sökbegrepp får inte beskriva meddelandets innehåll. Användning av sökbegrepp som beskriver meddelandets innehåll kan anses innebära ett kraftigare ingripande i skyddet för utomståendes förtroliga kommunikation, eftersom verksamheten förutsätter att all kommunikation som är föremål för filtrering öppnas på datateknisk väg för att det ska klarläggas huruvida innehållet motsvarar sökbegreppet. Innehållet i ett meddelande har av hävd ansetts utgöra kärnområdet i hemligheten för förtroliga meddelanden.

Det föreslås emellertid två noggrant avgränsade undantag från förbudet mot att använda sökbegrepp som beskriver meddelandets innehåll. För det första får sökbegrepp som beskriver innehållet användas när underrättelseinhämtning som avser datatrafik kan inriktas så att den omfattar enbart en främmande stats eller en med en sådan jämställbar parts datatrafik (68 §), alltså datatrafiken för en sådan aktör som inte åtnjuter skydd för hemligheten för ett förtroligt meddelande. Undantaget tillämpas bara om det i det datatrafikflöde i vilket sökbegrepp används inte förekommer någon utomstående kommunikation som åtnjuter skydd för hemligheten för ett förtroligt meddelande.

Det andra undantaget gäller sabotageprogram och skadliga kommandon. Sökbegrepp som beskriver innehållet i ett sabotageprogram eller ett skadligt kommando är olika tekniska teckensträngar, inte ord eller uttryck i ett naturligt språk. På grund av särarten hos sökbegrepp som gäller sabotageprogram kan de användas som sökbegrepp som avser meddelandets innehåll.

Försvarsmaktens underrättelsetjänst kan inte fritt välja sökbegrepp eller kategorier av sökbegrepp medan en metod för underrättelseinhämtning används, i stället ska sökbegreppen listas i domstolsbeslutet.

I människorättsdomstolens avgörandepraxis har tillståndsbeslut som en domstol fattat ansetts vara en viktig rättsskyddsgaranti, om en åtgärd ingriper i skyddet för förtroliga meddelanden. Ärenden om underrättelseinhämtning som avser datatrafik föreslås bli behandlade vid Helsingfors tingsrätt, alldeles som de andra metoder för underrättelseinhämtning som förutsätter domstolsbehandling.

Domstolen föreslås kunna bevilja tillstånd för högst sex månader åt gången.

Det är meningen att filtreringen inte i ett enda enskilt fall där underrättelseinhämtning som avser datatrafik används ska omfatta all datatrafik som överskrider Finlands gräns i ett kommunikationsnät. Användningen av underrättelseinhämtning som avser datatrafik förutsätter att Försvarsmaktens underrättelsetjänst känner till eller misstänker en konkret förekomst av ett föremål för militär underrättelseinhämtning och fakta kring detta. Föremålets art vid tidpunkten i fråga och de fakta om föremålet som är kända inverkar på i vilken del av ett kommunikationsnät datatrafiken kan antas överskrida Finlands gräns. Exempelvis kan man anta att

främmande statliga aktörers datatrafik överskrider gränsen i andra delar av ett kommunikationsnät än de som används för utbyte av meddelanden mellan andra aktörer. Som ovan framgår kan det anses att underrättelseinhämtning som avser datatrafik inte handlar om underrättelseinhämtning som riktas mot all tänkbar datatrafik, s.k. massövervakning.

Genomförandet av underrättelseinhämtning som avser datatrafik förutsätter att en accesspunkt har byggts i den del av kommunikationsnätet som överskrider gränsen. Principen är att byggandet av accesspunkter ska ske med medverkan av de företag som äger eller innehar gränsöverskridande delar av ett kommunikationsnät (94 §). Dessutom är en part som äger eller innehar en kommunikationsnätsdel som överskrider Finlands gräns skyldig att ge de data som den förfogar över för att det ska kunna bedömas i vilken del av kommunikationsnätet datatrafik från en viss plats kommer att routas över Finlands gräns (95 §).

Efter att domstolen har beviljat tillstånd till underrättelseinhämtning som avser datatrafik kopplar den som utför kopplingen Försvarsmaktens underrättelsetjänsts system för underrättelseinhämtning som avser datatrafik till datatrafiken i den kommunikationsnätsdel som tillståndet avser (69 §). Genom kopplingen styrs datatrafiken i den kommunikationsnätsdel som tillståndet avser så att det filtreras. Suomen Erillisverkot Oy eller ett dotterbolag som det heläger utför kopplingen och överlåter den i tillståndet avsedda datatrafiken. Uppdraget anvisas en part som är oberoende av underrättelsemyndigheterna för att det ska säkerställas att underrättelsemyndigheterna inte får mer omfattande åtkomst till datatrafiken än vad som tillåts i det av domstolen meddelade tillståndsbeslutet.

Rätten för Försvarsmaktens underrättelsetjänst att uppta information som inhämtats med hjälp av underrättelseinhämtning som avser datatrafik samt utplåningen av information som upptagits och utlämnandet av uppgifter ur datasystemet grundar sig på bestämmelserna om behandling av uppgifter. Längre fram i lagen föreslås särskilda bestämmelser om sådana särskilda förbud mot underrättelseinhämtning som begränsar användningen av underrättelseinhämtning som avser datatrafik och bestämmelser om en skyldighet att utan dröjsmål utplåna viss information som erhållits med underrättelseinhämtning som avser datatrafik (7 kap.). De föreslagna förbuden mot underrättelseinhämtning och skyldigheterna att utplåna information begränsar i betydande utsträckning vilken med denna metod erhållna information som får sparas i Försvarsmaktens underrättelsetjänsts datasystem.

I kapitlet om metoder för underrättelseinhämtning föreskrivs det också om tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning (70 §). Det tekniska genomförandet omfattar en statistisk analys på uppdrag av skyddspolisen och informationsinhämtning för skyddspolisen i enlighet med ett tillstånd som domstolen har beviljat skyddspolisen. I det senare fallet får Försvarsmaktens underrättelsetjänst inte tillgång till den inhämtade datatrafikens innehåll, utan det är endast fråga om insamling av datatrafik och vidareöverlåtelse av den till skyddspolisen.

Förslaget innebär att underrättelseinhämtning som avser datatrafik inte ska användas för underrättelseinhämtning i fråga om datatrafik som rör sig i Finlands interna kommunikationsnät eller datatrafik mellan parter som befinner sig i Finland. I det sistnämnda fallet kan datatrafiken emellertid routas från avsändaren till mottagaren via en gränsöverskridande del av ett kommunikationsnät. Dessutom är det ändamålsenligt att underrättelseinhämtning som avser datatrafik inte ska omfatta sådan kommunikation som parten har skyldighet eller rätt att vägra vittna om. Eftersom sökbegrepp som avser de ovannämnda fallen inte kan genomföras tekniskt vid underrättelseinhämtning som avser datatrafik, föreskrivs det i lagen separat om en skyldighet att utplåna information (81 §). Försvarsmaktens underrättelsetjänst ska i sådana fall

utplåna informationen omedelbart efter att det framgått att kommunikationen försiggick mellan två parter som befinner sig i Finland.

*Skyddande av militär underrättelseinhämtning samt tryggande av tjänstemän och informationskällor (5 kap.)*

I kapitlet föreskrivs det om skyddande av militär underrättelseinhämtning (72–73 §). Enligt förslaget får militärunderrättelsemyndigheten använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt upprätta och använda falska handlingar, när det behövs för att förhindra att den militära underrättelseinhämtningen avslöjas.

Skyddandet täcker hela den militära underrättelseverksamheten och möjliggör därmed ett mer omfattande skydd för verksamheten än gällande lagstiftning om andra myndigheters befogenheter. Skyddandet får inte företas lättvindigt, eftersom olika problem och rättsskyddsaspekter hänger samman med det. Därför bör skydd tillgripas först när det är nödvändigt.

I kapitlet finns också bestämmelser om tryggande av tjänstemän som är anställda hos militärunderrättelsemyndigheten och utför förtäckt inhämtande av information, täckoperationer eller bevisprovokation genom köp (74 §). Att trygga tjänstemän föreslås vara möjligt också i en situation där militärunderrättelsemyndigheten förbereder eller genomför användning av informationskällor.

En föreslagen bestämmelse som inte finns i gällande polislag handlar om tryggande av informationskällor (75 §). Enligt förslaget kan militärunderrättelsemyndigheten med en informationskällas samtycke övervaka dennes bostad eller ett annat utrymme som informationskällan använder och dess omedelbara närmiljö med kamera eller en annan teknisk anordning, metod eller programvara som installerats på platsen, om det är nödvändigt för att avvärja en fara som hotar informationskällans liv eller hälsa.

Användningen av informationskällor är mycket sensitiv verksamhet och kan inbringa detaljerade uppgifter om föremålet för militär underrättelseinhämtning. Tryggandet av en informationskällas liv och hälsa kan vara en förutsättning för att militärunderrättelsemyndigheten ska få tillgång till dessa uppgifter. Bestämmelsen möjliggör också att informationskällan ges falska, vilseledande och förtäckta uppgifter eller registeranteckningar eller att falska handlingar upprättas för att användas av informationskällan. Förutsättningen är att detta är nödvändigt för att få uppgifter med tanke på ett underrättelseuppdrag samt för att skydda informationskällans liv och hälsa.

*Utlämnande av underrättelseuppgifter i vissa fall (6 kap.)*

I 6 kap. föreskrivs det om utlämnande av militära underrättelseuppgifter i vissa fall. Det kan i vissa fall vara fråga om en skyldighet att underrätta förundersökningsmyndigheten eller den brottsbekämpande myndigheten. Det handlar om ett undantag från ändamålsbundenheten för information som erhållits med metoder för underrättelseinhämtning. Under vissa förutsättningar som anges i 76 eller 77 § kan uppgifter som erhållits med en metod för underrättelseinhämtning anmälas till förundersökningsmyndigheten eller den brottsbekämpande myndigheten.

Regleringen om detta har utarbetats så, att det i den på ett balanserat sätt beaktas att ändamålet för underrättelseinhämtning inte är brottsbekämpning och att ett stort samhällsintresse är för-

knippat med att allvarliga brott utreds och framför allt förhindras. Anmälan av lindriga brott som framkommit vid underrättelseinhämtning får inte vara automatisk i den bemärkelsen att underrättelseinhämtningen de facto blir ett sätt att förhindra och reda ut sådana brott. Samtidigt bör det vara möjligt att anmäla också förhållandevis lindriga brott till den brottsbekämpande myndigheten, om detta från fall till fall är nödvändigt för att fullfölja underrättelseinhämtningens syfte. Utredning och särskilt förhindrande av de allra allvarligaste brotten åter är förenligt med samhällets totalintresse, vilket är anledningen till att det är befogat att i stor utsträckning tillåta att de anmäls till brottsbekämpningen. För anmälan talar också rättviseaspekten och hänsynstagandet till den syn på saken som offren för allvarliga brott anlägger.

Vidare är det meningen att uppgifter som erhållits med en metod för underrättelseinhämtning ska kunna anmälas till enskilda aktörer i vissa fall (77 §). I kapitlet finns också bestämmelser om anmälan om att förundersökning eller brottsbekämpning inleds (77 §).

*Förbud mot underrättelseinhämtning, utplåning av underrättelseinformation och underrättelse om att en metod för underrättelseinhämtning används (7 kap.)*

Kapitlet innehåller bestämmelser om förbud mot underrättelseinhämtning (79–80 §). I enlighet med vad som anges i allmänna motiveringen kan det inte vara acceptabelt att militär underrättelseverksamhet riktas mot vissa parter i särställning.

Paragrafen om utplåning av underrättelseinformation (81 §) gäller vissa metoder för underrättelseinhämtning. Paragrafen kompletteras av särskilda bestämmelser om avbrytande och utplåning som gäller användning av vissa metoder för underrättelseinhämtning (82–83 §). Utplåning av uppgifter som fåtts i en brådskande situation (84 §) omfattar alla metoder för underrättelseinhämtning för vars del det föreskrivs om ett brådskande förfarande.

I 85 § föreskrivs det om användning av en uppgift som inte ansluter sig till ett underrättelseuppdrag.

Paragrafen om underrättelse om användning av en metod för underrättelseinhämtning (86 §) motsvarar i stor utsträckning det som i 5 kap. 58 § i polislagen föreskrivs om underrättelse om hemligt inhämtande av information.

*Deltagande av en annan tjänsteman vid Försvarsmakten och av värnpliktiga i militär underrättelseinhämtning samt internationell verksamhet (8 kap.)*

Även andra tjänstemän vid Försvarsmakten än sådana som är i tjänst hos militärunderrättelsemyndigheten har kompetens som är väsentlig med tanke på underrättelseinhämtningen (87 §). Denna kompetens föreslås kunna utnyttjas endast under militärunderrättelsemyndighetens ledning, styrning och tillsyn.

Det föreslås att reservister som har fått tillräcklig utbildning ska kunna delta i vissa fall i utförandet av underrättelseuppdrag under militärunderrättelsemyndighetens styrning och övervakning (88 §). Inom den militära underrättelseinhämtningen bör reservister också kunna användas redan före en mobilisering, för att effektivisera beredskapen.

Eftersom de viktigaste aktörerna i den organisation som deltar i Försvarsmaktens internationella operationer är reservister föreslås särskilda bestämmelser om deras befogenheter i sådana uppdrag (89 §). I lagen regleras också situationer där en person som gått i pension från mili-

tärunderrättelsemyndigheten kan besluta om användningen av metoder för underrättelseinhämtning inom Försvarsmaktens internationella verksamhet.

I kapitlet föreskrivs dessutom om tjänsteansvar respektive skadeståndsansvar (90 respektive 91 §) för den som tjänstgör i enlighet med värnpliktslagen.

*Yppandeförbud, skyldigheter och rättigheter som gäller teleföretag och dataöverförare samt användning och erhållande av information (9 kap.)*

När en metod för underrättelseinhämtning används är det möjligt att råka i en situation där utomstående hjälp behövs eller rentav är nödvändig. Därför föreskrivs det i kapitlet om yppandeförbud för utomstående som har bistått vid militär underrättelseinhämtning och om en möjlighet för militärunderrättelsemyndigheten att få information av privata sammanslutningar (92 §). Ett beslut om yppandeförbud omfattas av besvärsförbud och får inte överklagas genom besvär, enligt förslaget. Den som har meddelats ett förbud får dock utan tidsfrist anföra klagan över beslutet. Klagan ska behandlas skyndsamt. Underrättelseombudsmannen ska alltid informeras om beslut om yppandeförbud (105 §).

Därtill föreskrivs det i kapitlet om skyldigheter för teleföretag och dataöverförare samt om ersättningar till dem och till den som utför kopplingar (93–99 §). De ovannämnda parterna är i en central ställning när det gäller att använda metoder för underrättelseinhämtning som riktas mot kommunikationsnät. Dessutom föreskrivs det om rätten att få information av privata sammanslutningar (101 §).

*Övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen (10 kap.) och särskilda bestämmelser (11 kap.)*

I 10 kap. föreskrivs det om den interna övervakningen av militär underrättelseverksamhet inom försvarsförvaltningen. Med intern övervakning avses den övervakning av verksamheten som sker inom Försvarsmakten och övervakning som försvarsministeriet utför. Separata bestämmelser föreslås i fråga om extern laglighetsövervakning och parlamentarisk övervakning.

Dessutom föreskrivs det om förfarandet i domstol (113 §). Ärenden som gäller militär underrättelseinhämtning ska enligt förslaget behandlas vid Helsingfors tingsrätt. Eftersom Helsingfors tingsrätt har landets bredaste erfarenhet av att behandla ärenden om hemlig informationsinhämtning och hemliga tvångsmedel kan det anses att den har tillräcklig specialkompetens också i ärenden om metoder för underrättelseinhämtning.

*Övriga lagförslag*

Det föreslås att en hänvisningsbestämmelse till lagen om militär underrättelseverksamhet fogas till lagen om försvarsmakten.

Målet är att göra tydlig åtskillnad mellan förundersökning som Försvarsmakten utför och militär underrättelseinhämtning. Till lagen om militär disciplin och brottsbekämpning inom försvarsmakten föreslås bli fogade bestämmelser om att tjänstemän vid militärunderrättelsemyndigheten, dvs. Försvarsmaktens underrättelsetjänst och Huvudstabens underrättelseavdelning, inte ska ha en disciplinär förmans befogenheter som det föreskrivs om i den lagen. Det innebär att de inte ska kunna ha hand om förundersökningsuppgifter eller utöva befogenheter med anknytning till förundersökning. Förundersökningen av ett brott som misstänks ha begåtts av en tjänsteman vid Försvarsmaktens underrättelsetjänst ska enligt den föreslagna regleringen för-

rättas av Huvudstaben. De som sköter förundersökning och utövar anknytande befogenheter ska uttryckligen vara tjänstemän vid Huvudstabens juridiska avdelning.

Lagen om verksamheten i den offentliga förvaltningens säkerhetsnät föreslås bli ändrad så, att ett dotterbolag till Suomen Erillisverkot Oy får ha även andra uppgifter än sådana som hänför sig till verksamheten i säkerhetsnät, om bestämmelser om detta finns någon annanstans i lag. Med detta hänvisas det bl.a. till den i lagen om militär underrättelseverksamhet föreskrivna uppgiften att vara den som utför en koppling, enligt definitionen i 9 § 1 punkten i den lagen.

Till inkomstskattelagen (1535/1992) fogas en ny bestämmelse enligt vilken som skattepliktig inkomst inte betraktas ett av en myndighet utbetalt arvode till en informationskälla som avses i lagen om militär underrättelseverksamhet och polislagen för inhämtning av information som är av betydelse för skötseln av underrättelseuppdrag.

## 4 Propositionens konsekvenser

### 4.1 Ekonomiska konsekvenser

#### 4.1.1 Konsekvenser för de offentliga finanserna

Propositionens konsekvenser för de offentliga finanserna hänför sig särskilt till Försvarsmaktens nya befogenheter. Propositionen medför också övriga kostnader för tillståndsmyndigheten och för försvarsministeriet i och med de resurser som det fördjupade samarbetet mellan myndigheterna kräver.

Totalt sett kan den information som fås genom militär underrättelseverksamhet uppskattas effektivisera Försvarsmaktens resursanvändning och hela samhällets beredskap för olika typer av hot. Aktuell information om strategiska, taktiska och operativa planer och verksamhetsmodeller ger bättre möjligheter till beredskap inför hot på det effektivaste och bästa möjliga sättet. De ekonomiska fördelarna tillfaller såväl Försvarsmakten, i fråga om t.ex. bättre inriktade upphandlingar och utbildningar, som hela samhället t.ex. i och med att hot och deras konsekvenser kan förebyggas.

##### 4.1.1.1 Underrättelseinhämtning som avser datatrafik

Driftskostnaderna för den koppling som underrättelseinhämtning som avser datatrafik förutsätter uppskattas medföra tilläggskostnader på cirka 700 000 euro per år för Försvarsmakten från och med 2019.

Under 2019 uppskattas befogenheterna för underrättelseinhämtning som avser datatrafik medföra tilläggskostnader på cirka 1,2 miljoner euro för Försvarsmakten. Kostnaderna består av ersättningar till företag av de kostnader som underrättelseinhämtning som avser datatrafik medför samt av hyror för utrustning och serverhallar och andra verksamhetskostnader som denna underrättelseinhämtning medför. År 2020 uppskattas kostnaderna för underrättelseinhämtning som avser datatrafik uppgå till 1,7 miljoner euro, varefter de ökar med 0,5 miljoner euro årligen fram till 2022.

De administrativa kostnaderna och omkostnaderna uppskattas medföra tilläggskostnader på cirka 350 000 euro år 2018, varefter tilläggskostnaderna uppskattas till cirka 1,1 miljoner euro per år. Detta inbegriper kostnaderna för underrättelseinhämtning som avser datatrafik för skyddspolisens räkning.

I övrigt kan de systeminvesteringar och personalresurser som underrättelseinhämtning som avser datatrafik förutsätter fördelas som Försvarsmaktens normala verksamhet inom ramen för utvecklingsprogrammen.

I det inledande skedet medför utförandet av en koppling kostnader på uppskattningsvis 500 000 euro årligen. I takt med att verksamheten utvecklas uppgår kostnaderna, som orsakas av lokalhyror och arbete med anknytning till kopplingen, till 900 000 från och med år 2023. Inledandet av verksamheten medför dessutom anläggningskostnader på cirka 500 000 euro när lagen träder i kraft.

4.1.1.2 Operativa personalkostnader

Ett effektivt utnyttjande av de nya befogenheterna förutsätter att den operativa informationsinhämtningen förstärks genom utökade personalresurser och systemutveckling. Då mängden rådata som militärunderrättelsemyndigheten inhämtar ökar till följd av de nödvändiga satsningarna bör man säkerställa möjligheten att utnyttja informationen genom att satsa på tekniska och operativa analyser och förbehandling av informationen samt på fortsatt utredning av hoten. För att man ska kunna effektivisera informationsinhämtningen och utnyttja den inhämtade informationen för skötseln av militärunderrättelsemyndighetens uppgifter förutsätts det att militärunderrättelsemyndigheten ytterligare utvidgar sitt samarbetsnätverk genom att skapa nya partnerskap med inhemska och utländska myndigheter och andra aktörer. Därför kommer det operativa samarbetet att öka avsevärt.

Den uppskattade tilläggskostnaden för 2019 är en miljon euro, varefter kostnaderna ökar med en miljon euro per år fram till 2021. Kostnaderna beror på inrättandet av nya permanenta tjänster. Ett effektivt och fullskaligt utnyttjande av befogenheterna till underrättelseinhämtning förutsätter att utvecklingen av taktiska och tekniska metoder inleds i god tid före ikraftträdandet av lagen och att den operativa personalen har fått tillräcklig utbildning i användningen av befogenheterna före ikraftträdandet. Av denna anledning bör nya tjänster inrättas och nya metoder utvecklas delvis redan innan lagen träder i kraft 2018. Tilläggskostnaderna uppskattas då till 600 000 euro.

4.1.1.3 Övriga befogenheter

Införandet av nya befogenheter förutsätter att man utvecklar de metoder, anordningar, system och analysfunktioner som militärunderrättelsemyndigheterna använder. För att informationsinhämtningen enligt de nya befogenheterna ska kunna utvecklas och den inhämtade informationen ska kunna utnyttjas på ett säkert sätt krävs att man skaffar den utrustning som behövs och bygger upp systemen med framförhållning. Detta förutsätter en tilläggsfinansiering på 3,4 miljoner euro för 2018. Driftskostnaderna för användningen av befogenheterna och för systemen uppskattas medföra tilläggskostnader på cirka 800 000 euro under 2019 och därefter 1,1 miljoner euro från och med 2020.

De befogenheter som inte gäller underrättelseinhämtning som avser datatrafik medför dessutom ökade administrativa kostnader och omkostnader för exempelvis utbildning eller tillsynsrelaterade anmälningar till underrättelseombudsmannen. Tilläggskostnaderna under 2018 då verksamheten inleds uppskattas till cirka 450 000 euro, varefter de årliga tilläggskostnaderna uppgår till cirka 900 000 euro år 2019 och från och med 2020 till 1,5 miljoner euro.

De nya befogenheterna förutsätter specialutbildad personal, skydd för informationsinhämtningen och personalen samt vid behov jour dygnet runt. Kostnaderna beror på den ökade per-

sonalstyrkan, som inte har beaktats i utvecklingsprogrammen eller budgetramarna inom Försvarsmakten. Ökningen i personalstyrkan uppskattas medföra ett behov av ett tilläggsanslag på cirka 1,6 miljoner euro när lagen träder i kraft, och i takt med att den militära underrättelseverksamheten utvecklas uppskattas kostnaderna till cirka 2,6–3,6 miljoner euro per år.

Kostnaderna för underrättelseinhämtning som avser utländska datasystem och radiosignalspaning kan täckas inom ramen för utvecklingsprogrammen inom Försvarsmakten.

4.1.1.4 Beslutsfattande, kommunikation, styrning och tillsyn avseende underrättelseverksamhet inom försvarsministeriets förvaltningsområde

Den interna tillsynen av den militära underrättelseverksamheten förutsätter tilläggsresurser vid huvudstaben. Den tekniska övervakningen och laglighetsövervakningen inom underrättelseverksamheten bör organiseras så att den är effektiv, fungerande och trovärdig. Tilläggsresurser motsvarande sex årsverken bör anvisas för den interna laglighetsövervakningen. De nya uppgifterna uppskattas medföra ytterligare personalkostnader på cirka 320 000 euro (4 årsv.) år 2018, varefter tilläggskostnaderna uppskattas till cirka 480 000 euro (6 årsv.) per år. Tillsynen av underrättelseverksamheten medför dessutom tilläggskostnader som beror på omskolning av personal till nya uppgifter.

I samband med beredningen av lagstiftningen om militär underrättelseverksamhet och i och med att samhällets förväntningar ökar finns det tecken på ett ökat behov av att så öppet som möjligt informera om frågor som gäller den militära underrättelseverksamheten. Produkter avsedda för militär underrättelseinhämtning är i regel klassificerade för myndighetsbruk eller lägre skyddsnivå, och offentlig spridning av dem kräver särskilt kunnande. Det uppskattas att dessa uppgifter förutsätter tilläggsfinansiering på cirka 140 000 euro (2 årsv.) från och med 2019.

Samarbetet inom den militära underrättelseinhämtningen med andra myndigheter och den högsta statsledningen samt styrningen av den militära underrättelseverksamheten ger upphov till tilläggskostnader för försvarsministeriet. Till följd av detta behövs en tilläggsresurs motsvarande ett årsverke vid ministeriet. De huvudsakliga uppgifterna för den som sköter den tilltänkta tjänsten omfattar beredning av politiskt beslutsfattande som gäller militär underrättelseverksamhet, planering av verksamheten och resurserna samt utveckling av samarbetet nationellt och internationellt. Tjänsten bör inrättas redan innan lagen träder i kraft så att styrningen av verksamheten och samarbetet med andra myndigheter är adekvat när den militära underrättelseverksamheten inleds. De årliga kostnaderna för tjänsten uppskattas till cirka 90 000 euro från och med 2018.

Innan lagen träder i kraft bör man kontrollera att det finns tillräckliga resurser för laglighetsövervakning vid försvarsministeriet. De föreslagna nya uppgifterna med anknytning till laglighetsövervakning medför ett behov av ett ytterligare årsverke vid försvarsministeriet. Den huvudsakliga uppgiften för den tilltänkta tjänsten är att övervaka lagligheten i den militära underrättelseverksamheten. Uppgifterna omfattar dessutom annan övervakning av lagligheten inom ministeriet och förvaltningsområdet, rapportering till tillsynsorganen och samarbete kring laglighetsövervakningen inom förvaltningsområdet. De årliga kostnaderna för tjänsten uppskattas till cirka 90 000 euro från och med 2018.

4.1.1.5 Ekonomiska konsekvenser för andra myndigheter

Den domstol som ät tillståndsmyndighet för användningen av befogenheter orsakas tilläggskostnader i och med det ökade antalet ärenden som ska behandlas. Byggandet av lokaler och informationssystem som är tillräckligt informationssäkra för att tillståndsärenden som gäller underrättelseverksamhet ska kunna behandlas i dem medför också kostnader. Vid behov kan även Försvarsmaktens säkerhetsutrymmen användas. Användningen av de föreslagna befogenheterna uppskattas medföra tilläggskostnader på cirka 100 000 euro för justitieministeriets förvaltningsområde.

Enligt en uppskattning från Helsingfors tingsrätt binder behandlingen av tvångsmedelsärenden upp domarresurser motsvarande en cirka tre månaders arbetsinsats. I brottmål varierar arbetsmängden avsevärt beroende på ärendets omfattning. De mest omfattande och arbetskrävande ärendena behandlas vanligen i en sammansättning på tre domare. Ytterst omfattande ärenden kan till och med behandlas i flera år. Lagstiftningen om militär underrättelseverksamhet uppskattas leda till ett ärende per år som är mer omfattande än normalt. Om ärendet är så omfattande att det behandlas i tingsrätten i tre månader förutsätter det i en sammansättning på tre domare en domarresurs på sammanlagt nio månader. Tvångsmedelsärenden och brottmål kan uppskattas binda upp en resurs motsvarande sammanlagt ett domarårsverke, vilket förutsätter en ökning av omkostnadsanslaget med 80 000 euro under omkostnadsmomentet för övriga domstolar 25.10.03.

De som begär information av militärunderrättelsemyndigheten orsakas mindre tilläggskostnader, t.ex. för översättning. Anmälningsskyldigheten och anmälningsrätten medför administrativa kostnader för förundersökningsmyndigheten och brottsbekämpningsmyndigheten. Det uppskattas att kostnaderna inte blir betydande, eftersom anmälningsförfarandet på grund av den militära underrättelseinhämtningens natur sällan kommer att tillämpas.

Adekvat beredskap för hot som den militära underrättelseverksamheten identifierat kan medföra kostnader inom olika förvaltningsområden, t.ex. i form av ökade anslag för utbildning i att förebygga konsekvenserna av informationspåverkan. Det är inte möjligt att bedöma dessa konsekvenser på förhand, eftersom hoten kan vara av ytterst varierande slag.

4.1.1.6 Helhetsbedömning

Den totala tilläggskostnaden av de nya myndighetsuppgifterna för försvarsministeriets förvaltningsområde uppskattas till cirka 10 miljoner euro på årsnivå när verksamheten inleds. Propositionen beräknas dessutom medföra ekonomiska konsekvenser på 5,3 miljoner euro under 2018, inklusive engångsanskaffningar.

| Sammandrag av lagförslagets ekonomiska konsekvenser för försvarsförvaltningen | **S2018** | **S2019**<br><br>(lagen uppskattas träda i kraft) | **S2020** | **S2021->** |
|---|---|---|---|---|
| **Engångsinvesteringar** | | | | |

| | | | | |
|---|---|---|---|---|
| kostnader för utrustning och informationssystem | 3 400 000 | - | - | - |
| **Personalkostnader (Försvarsmakten)** | | | | |
| operativa | 600 000 | 1 000 000 | 2 000 000 | 3 000 000 |
| intern övervakning (årsv.) | 320 000 (4 årsv.) | 480 000 (6 årsv.) | 480 000 (6 årsv.) | 480 000 (6 årsv.) |
| kommunikation | | 140 000 (2 årsv.) | 140 000 (2 årsv.) | 140 000 (2 årsv.) |
| **Personalkostnader (Försvarsministeriet)** | | | | |
| styrning och uppföljning (årsv.) | 90 000 (1 årsv.) | 90 000 (1 årsv.) | 90 000 (1 årsv.) | 90 000 (1 årsv.) |
| laglighetsövervakning (årsv.) | 90 000 (1 årsv.) | 90 000 (1 årsv.) | 90 000 (1 årsv.) | 90 000 (1 årsv.) |
| **Övriga årliga kostnader totalt** | | | | |
| *Underrättelseinhämtning som avser datatrafik* | | | | |
| hyror för utrustning och serverhallar som behövs för kopplingen, ersättningar till företag | - | 1 200 000 | 1 700 000 | 2 200 000 |
| administrativa kostnader och omkostnader | 350 000 | 1 100 000 | 1 100 000 | 1 100 000 |
| driftskostnader för kopplingen | - | 700 000 | 700 000 | 700 000 |
| hyror för utrustning och serverhallar som behövs för systemet för underrättelseinhämtning som avser datatrafik | - | 700 000 | 1 400 000 | 2 100 000 |
| underhåll av systemet för underrättelseinhämtning som avser datatrafik | - | 1 000 000 | 1 000 000 | 1 000 000 |
| kostnader för inledande av verksamheten för den som utför en koppling | - | 500 000 | - | - |
| arbete, utrustningsinvesteringar och lo- | - | 500 000 | 600 000 | 700 000 |

| | | | | |
|---|---|---|---|---|
| kalhyror i samband med en koppling | | | | |
| informationssäkerhet | - | 500 000 | 1 000 000 | 1 000 000 |
| *Övriga befogenheter* | | | | |
| underhåll av utrustning och informationssystem | - | 800 000 | 1 100 000 | 1 100 000 |
| administrativa kostnader och omkostnader, inkl. utbildning | 450 000 | 900 000 | 1 500 000 | 1 500 000 |
| lokalhyror | - | 250 000 | 250 000 | 250 000 |
| **Totalt** | 5 300 000 | 9 950 000 | 13 150 000 | 15 450 000 |

Den slutliga tidpunkten för när de ovannämnda tilläggskostnaderna utfaller och vilka år de gäller beror på när de föreslagna bestämmelserna träder i kraft.

Tilläggskostnaderna kan inte täckas inom ramen för de nuvarande årliga anslagen för försvarsministeriets förvaltningsområde. Behovet av tilläggsfinansiering kommer att presenteras i tilläggsbudgeten för 2018 och i planen för de offentliga finanserna för 2019–2022.

De kostnadseffekter som nämns ovan 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.

4.1.2 Konsekvenser för samhällsekonomin och för företag

Underrättelselagstiftningens konsekvenser för företagen, samhällsekonomin och näringslivet bör bedömas som en helhet. Bedömningen av lagstiftningens konsekvenser bör göras med beaktande av i synnerhet digitaliseringsutvecklingen i samhället och företagens verksamhetsförutsättningar, eftersom det med tanke på den ekonomiska tillväxten är nödvändigt att Finland effektivt utnyttjar de möjligheter till att förändra verksamhetssätten och förbättra produktiviteten som informations- och kommunikationstekniken medför.

Lagstiftningen om militär underrättelseverksamhet syftar till att skydda Finland samt landets nationella säkerhet och samhällsekonomi. Det centrala målet för lagstiftningen om militär underrättelseverksamhet är att inhämta information om hot mot intressen som är väsentliga för Finlands nationella säkerhet och hot mot samhällsekonomin samt att förebygga dessa. Utvecklingen av underrättelselagstiftningen kan således bedömas höja tröskeln för utländska makter att bedriva spionerі eller andra skadliga aktiviteter via datanäten mot Finland. En utökning av underrättelsekapaciteten minskar dock inte behovet för sammanslutningar eller individer att vidta egna skyddsåtgärder eller vikten av dessa, utan de är fortfarande de centrala metoderna när det gäller att skydda sig mot olika hot. En fungerande reglering och en utökad kapacitet kompletterar dock säkerheten i den digitala miljön i Finland och främjar näringslivets

möjligheter att skydda sig mot hot från främmande makter. Viktigt i detta avseende är t.ex. att information som inhämtats genom metoder för underrättelseinhämtning vid behov kan lämnas ut till företag för att avvärja allvarliga hot eller försvara viktiga ekonomiska intressen.

Med tanke på samhällsekonomin och verksamhetsförutsättningarna för de företag som är en del av den är det viktigt att den rättsgrund som skapas i Finland för underrättelsemyndigheternas verksamhet är tydlig. En tillräckligt exakt och balanserad lagstiftning skapar en förutsägbarhet som gör att företagen kan planera sin verksamhet och fatta investeringsbeslut. När dataskyddet och lagstiftningen om underrättelseverksamheten får större betydelse på den digitala marknaden kan en exakt, rättvis och proportionell reglering i bästa fall uppskattas vara en positiv konkurrensfaktor för Finland på den internationella marknaden. Bland annat därför har strävan varit att utforma lagförslagen för att motsvara dessa kriterier.

För att man ska kunna identifiera hot mot samhället och bevara den kritiska infrastrukturen och samhällets ekonomiska livskraft krävs samarbete mellan den offentliga och den privata sektorn. Detta innebär ett smidigt informationsutbyte mellan underrättelsemyndigheterna och den privata sektorn. Lagförslaget syftar till att skapa en tillräcklig rättslig grund för att militärunderrättelsemyndigheterna ska kunna lämna ut information till företag för att skydda deras viktiga intressen. Underrättelseinformation kan vid behov lämnas ut till privata sammanslutningar för att göra det möjligt att avvärja allvarliga hot eller förhindra avsevärda ekonomiska förluster. Det aktuella förslaget innehåller bestämmelser om saken.

4.1.2.1 Administrativa och ekonomiska konsekvenser för företag

Propositionen bedöms ha en del konsekvenser för företag. Konsekvenserna riktar sig särskilt mot teleföretag och ägare av kommunikationsnät som överskrider Finlands gräns.

Av de befogenheter som föreslås för den militära underrättelseverksamheten orsakas företagen direkta och indirekta kostnader av de nya befogenheterna att inhämta telekommunikationsuppgifter och av underrättelseinhämtning som avser datatrafik. De nya befogenheterna och de skyldigheter att lämna ut uppgifter som åläggs företagen ökar deras administrativa kostnader.

Propositionen medför administrativa kostnader för företagen. Samtidigt som befogenheterna till informationsinhämtning ökar stiger företagens kostnader för myndighetsservice till följd av myndighetsförfrågningar, begäranden om information eller andra skyldigheter inom olika sektorer inom näringslivet. Kostnaderna för företagen kan dock inte anses öka i betydande grad, eftersom Försvarsmaktens nya befogenheter beräknas minska antalet förfrågningar som grundar sig på brottsbekämpning och förfrågningar som görs inom brottsbekämpningen i samband med handräckning från polisen.

De administrativa kostnader som de nya metoderna för inhämtning av telekommunikationsuppgifter orsakar teleföretagen kan inte anses öka i betydande grad, eftersom en del av de tillstånd för inhämtning av telekommunikationsuppgifter som söks på brottsbekämpningsgrunder blir underrättelsebaserade.

Teleföretagen ersätts för de kostnader som inhämtningen av telekommunikationsuppgifter medför på det sätt som föreskrivs i 299 § i lagen om tjänster inom elektronisk kommunikation, vilket redan är fallet i fråga om metoderna för inhämtning av telekommunikationsuppgifter.

Ägare av kommunikationsnät som överskrider Finlands gräns orsakas administrativa kostnader av den skyldighet att lämna uppgifter som hänför sig till underrättelseinhämtning som av-

ser datatrafik och av den accesspunkt som tillhandahålls i en del av ett kommunikationsnät som överskrider Finlands gräns.

Förfrågningar som görs på basis av den skyldighet att lämna uppgifter som underrättelseinhämtning som avser datatrafik förutsätter ökar inte nämnvärt de administrativa kostnaderna för ägare av kommunikationsnät som överskrider Finlands gräns. Skyldigheten att lämna uppgifter gäller uppgifter som kommunikationsnätets ägare redan innehar, och ägaren förutsätts inte vidta nya åtgärder för att inhämta uppgifter.

Genomförandet av tekniska lösningar för underrättelseinhämtning som avser datatrafik förutsätter att tekniska anordningar installeras i delar av det kommunikationsnät som överskrider Finlands gräns. För anordningarna behövs utrymmen i de lokaler som tillhör ägaren av kommunikationsnätsdelen. Dessutom kräver installationen och det kontinuerliga arbetet med att underhålla och utveckla anordningarna att de anställda hos kommunikationsnätets ägare deltar i syfte att minimera de negativa effekterna för kommunikationsnätets funktion och ägarens eller innehavarens affärsverksamhet. De direkta kostnaderna för dessa arbeten ska enligt förslaget ersättas delvis till dem som äger och innehar delar av kommunikationsnätet. Den som utför en koppling får dessutom en självkostnadsbaserad ersättning för de kostnader som verksamheten ger upphov till.

4.1.2.2 Konsekvenser för forskning och utveckling och för uppkomsten av ny företagsverksamhet

Ett effektivt och pålitligt underrättelsesystem förutsätter att myndigheterna investerar i den teknik och det kunnande som används i underrättelseverksamheten. De föreslagna befogenheterna till informationsinhämtning förutsätter investeringar i teknik och satsningar på säker produktutveckling. På grund av verksamhetens natur bör investeringarna göras med särskild hänsyn till säkerheten i den teknik som anskaffas och de försörjningsberedskapsfrågor som är väsentliga för systemens funktion. Likaså bör man beakta möjligheterna att utnyttja avtalsbaserad serviceproduktion, eftersom det oundvikligen blir nödvändigt att köpa in tekniskt kunnande och resurser även från den privata sektorn. I en miljö där den digitala tekniken utvecklas snabbt kan detta leda till att nya affärsmodeller, arbetstillfällen och kompetenser uppstår i Finland.

Myndigheternas teknikinvesteringar kan skapa gynnsamma möjligheter för vissa högteknologiska företag när det gäller att utveckla de tjänster och den teknik som säkerhetsmyndigheterna behöver.

4.1.2.3 Konsekvenser för den internationella konkurrenskraften

Näringslivet agerar i en global miljö av internationell ekonomi och värdenätverk. I den globala konkurrensen påverkar även små faktorer staternas konkurrenskraft. Företagen etablerar sina verksamheter i olika länder för att optimera hela sin företagsverksamhet utifrån företagsspecifika konkurrensfördelar. Etableringsbeslut bygger på helhetsbedömningar med avseende på företagens affärsverksamhet, där man beaktar marknadsfaktorer såsom beskattningen, tillgången till energi, det teknologiska kunnandet, finländarnas höga utbildningsnivå, pålitlighet och ärlighet, arbetskraftsrelaterade skyldigheter, infrastrukturens och samhällets höga utvecklingsnivå, den samhälleliga och politiska stabiliteten, konsumentbeteendet och klimatmedvetenheten, den förutsägbara, stabila och noga avgränsade lagstiftningen, den administrativa bördan samt eventuella juridiska risker. Lagstiftningen är alltså en av åtskilliga faktorer som påverkar beslutsfattandet.

Näringsstrukturen i Finland har blivit servicecentrerad och ekonomin innovationsinriktad. Finland har gått över till kunskaps- och teknikintensiva branscher där det finns kluster som lockar utländska direkta placeringar. Informations- och kommunikationstekniken har kommit att bli ett särskilt styrkeområde för Finland. Den kunskapsintensiva industrins ekonomiska betydelse håller på att öka. Propositionens konsekvenser för företagsverksamheten varierar beroende på bl.a. vilken bransch företagen verkar i samt på deras storlek och den internationella verksamhet de bedriver.

En exakt, rättvis och proportionell lagstiftning förstärker Finlands rykte som ett land med ett förutsägbart och pålitligt företagsklimat. Detta gäller både aktörer som redan är verksamma i Finland och sådana som överväger att investera här.

Vid beredningen av propositionen har man bedömt lagstiftningens konsekvenser för Finlands internationella konkurrenskraft och för landets attraktionskraft som investeringsobjekt. Det väsentliga för IKT-sektorns konkurrenskraft är att regleringen inte förpliktar företagen att försämra tillförlitligheten i sina produkter eller tjänster t.ex. till följd av överlåtelse av krypteringsnycklar, installation av bakdörrar, begränsningar i användningen av kryptoprodukter eller andra skyldigheter som är skadliga för affärsverksamheten.

Med tanke på Finlands rykte bör det noteras att lagstiftningen inte ger underrättelsemyndigheten direkt och obegränsad tillgång till all datatrafik eller till innehållet i datalager som ägs av företag som är etablerade inom Finlands territorium. För att befogenheter som gäller integritetsskyddet ska kunna användas krävs ett tillståndsförfarande vid domstolen och behovet av användningen ska kunna motiveras på ett giltigt sätt och specificeras tillräckligt noggrant. Företagshemligheter skyddas genom lagens bestämmelser om behandlingsförbud och skyldighet att förstöra information samt om internationellt informationsutbyte mellan underrättelsemyndigheter.

I den preliminära beredningen av propositionen (arbetsgruppsbetänkandet Riktlinjer för en finsk underrättelselagstiftning) utreddes vilka negativa konsekvenser underrättelseinhämtning som avser datatrafik kan ha för utländska investeringar i Finland. Det konstaterades att konsekvenserna är svåra att bedöma, men Sverige, som har en synnerligen detaljerad och offentlig lagstiftning om underrättelseinhämtning som avser datatrafik, användes som jämförelseobjekt. I utredningen upptäcktes inga sådana avvikelser i den allmänna utvecklingen av de utländska investeringarna som kunde förklaras med inverkan från den svenska lagstiftningen om signalspaning. Enligt utredningen har ikraftträdandet av lagstiftningen om signalspaning ingen klar betydelse för utvecklingen i de utländska investeringarna i Sverige jämfört med investeringarna i Finland och Danmark. Sverige har t.ex. klarat sig bättre i jämförelsen Data Center Risk Index än Finland. Dessutom har Finland fortfarande fått nya datacenterinvesteringar medan lagstiftningsarbetet har pågått.

I dagsläget har myndigheterna begränsad kapacitet när det gäller att upptäcka statliga spionprogram eller spionoperationer som allvarligt kan skada den nationella säkerheten. Underrättelseinhämtning som avser datatrafik kan dock på ett betydande sätt komplettera Finlands möjligheter att skydda sig mot allvarliga hot från internet. Därmed gynnar underrättelseinhämtning som avser datatrafik även näringslivet när det gäller att skydda sig mot de allra allvarligaste hoten.

4.1.3 Konsekvenser för myndigheterna

De hot som kan identifieras med hjälp av militär underrättelseinhämtning är internationella, allvarliga och riktar sig mot statens viktiga säkerhetsintressen. De nya befogenheterna till militär underrättelseinhämtning kan ge information om utländska aktörer och omständigheter som är av betydelse för Finlands säkerhet och som stöder beslutsfattandet. De föreslagna befogenheterna ger den högsta statsledningen och Försvarsmaktens ledning bättre kapacitet att reagera på hot mot Finland.

Propositionen påverkar Försvarsmaktens uppgifter. I och med de nya befogenheterna utökas uppgiftsfältet för den militära underrättelseverksamheten och informationsinhämtningen ökar. I propositionen ställs höga kvalitativa, utbildningsmässiga och rättsliga krav för att lagen ska kunna verkställas.

Propositionen påverkar väsentligt förhållandena mellan myndigheterna. För det första förbättrar det informationstillskott som befogenheterna möjliggör militärunderrättelsemyndighetens förmåga att informera den högsta statsledningen om förändringar i Finlands säkerhetspolitiska omgivning. För det andra intensifieras samarbetet mellan militärunderrättelsemyndigheten och skyddspolisen i synnerhet inom underrättelseinhämtning som avser datatrafik, med beaktande av att dess tekniska genomförande ska koncentreras till Försvarsmaktens underrättelsetjänst. För det tredje kräver propositionen att relationerna mellan de interna och externa aktörerna inom övervakningssystemet för underrättelseverksamheten ses över helt, eftersom det enligt den lag om övervakning av underrättelseverksamheten som bereds vid justitieministeriet ska inrättas en helt ny myndighet för laglighetsövervakning inom underrättelseverksamheten.

Befogenheterna enligt den föreslagna regleringen ger Försvarsmakten en bättre förmåga att sköta sina lagstadgade uppgifter och de nya uppgifter som den åläggs i fråga om internationell handräckning.

Inom Försvarsmakten har propositionen betydande konsekvenser i synnerhet vad gäller arbetsvolymerna inom underrättelsesektorn. Propositionens mest omfattande konsekvenser för myndigheterna gäller militärunderrättelsemyndighetens uppgifter och förfaranden. De nya befogenheter som införs är av stor betydelse eftersom militärunderrättelsemyndighetens informationsinhämtning inte hänger samman med begreppet brott. Dessutom sträcker sig militärunderrättelsemyndighetens regionala behörighet över Finlands gränser. Denna uppgiftsförändring har konsekvenser för militärunderrättelsemyndighetens arbete med avseende på verksamheten, utbildningen, system- och metodutvecklingen och laglighetsövervakningen.

Propositionen förutsätter att det utvecklas ett utbildningssystem som motsvarar de nya uppgifterna. Grunden för användning av befogenheter inom den militära underrättelseverksamheten, de taktiska aspekterna av användningen, de nya befogenheterna och sättet på vilket underrättelseinhämtningsmetoderna inriktas avviker från de informationsinhämtningsmetoder som tilllämpas inom brottsbekämpningen. Därför krävs satsningar på utbildning och utveckling av verksamhetssätten.

Sådan underrättelseinhämtning som fokuserar på militära objekt som föreslås i propositionen torde endast sällan avslöja allvarliga brott som ger minst sex års fängelse, dvs. brott som måste anmälas till förundersökningsmyndigheten. Den föreslagna bestämmelsen om anmälan till brottsbekämpningen lär påverka förfarandena mer än uppgifterna gör det, liksom även hur och i vilken omfattning militärunderrättelsemyndigheten ska anmäla misstankar eller brott som ännu går att förhindra till förundersökningsmyndigheten.

I förslaget fördjupas det redan etablerade samarbetet mellan militärunderrättelsemyndigheten och skyddspolisen ytterligare genom en uttrycklig bestämmelse. Det fördjupade samarbetet mellan den militära och den civila underrättelseverksamheten innebär framför allt att man harmoniserar verksamhetssätten och ser till att underrättelseverksamheten inte riktas mot samma objekt. Samarbetet medför på längre sikt sannolikt också att militärunderrättelsemyndighetens och skyddspolisens operativa förfaranden och de rättsliga tolkningarna av dem blir mer enhetliga. Under vissa omständigheter kan samarbetet mellan militärunderrättelsemyndigheten och skyddspolisen även leda till att de delar utrustning och kunnande med varandra.

I den centraliserade lösningsmodell som presenteras i propositionen, där Försvarsmaktens underrättelsetjänst är den som tekniskt utför underrättelseinhämtning som avser datatrafik, gäller de resursmässiga konsekvenserna i första hand Försvarsmakten.

Enligt förslaget ska alla tillståndsärenden som gäller underrättelseinhämtningsmetoder behandlas i Helsingfors tingsrätt. Vid Helsingfors tingsrätt arbetar ett flertal tingsdomare som fokuserar på tvångsmedelsärenden, vilket gör att de kan specialisera sig på tillståndsärenden som gäller underrättelseinhämtningsmetoder och på frågor som gäller underrättelse om användning av sådana. Helsingfors tingsrätt åläggs också uppgifter som gäller underrättelse om användning av underrättelseinhämtningsmetoder, t.ex. att fatta beslut om att skjuta upp underrättelsen eller om att underrättelsen ska utebli helt. Tingsrättens arbetsvolym är således beroende av antalet yrkanden som gäller användning av underrättelseinhämtningsmetoder och undantag från huvudregeln om att den som varit föremål för sådana metoder ska underrättas. Då en tvångsmedelsdomare i genomsnitt kan avgöra 60 tillståndsärenden per månad har förslaget sannolikt inte någon större inverkan på arbetsvolymen vid Helsingfors tingsrätt. Även om de kvantitativa effekterna beräknas bli obetydliga ger skapandet av ett fungerande och effektivt joursystem upphov till kostnader.

Förslaget om att Helsingfors hovrätt ska vara den domstol där klagan över tillståndsärenden som gäller underrättelseinhämtningsmetoder anförs torde inte nämnvärt påverka arbetsvolymen vid hovrätten. Förslaget förutsätter dock att särskilt domarna vid Helsingfors tingsrätt utbildas med tanke på att yrkanden som gäller underrättelseinhämtningsmetoder måste motiveras på ett helt nytt sätt och att föremålen för den militära underrättelseverksamheten medför ett behov av bättre tolkningsförmåga.

Behandling av ärenden som gäller underrättelseverksamhet förutsätter lokaler med tillräckligt hög säkerhetsklassificering. Tillgången till sådana lokaler inom rättsväsendet måste säkerställas. Enligt förslaget kan ärenden också behandlas i försvarsförvaltningens lokaler.

På grund av underrättelseverksamhetens natur och för att verksamheten ska vara godtagbar krävs en ökad rättslig övervakning. För att säkerställa den externa laglighetsövervakningens oberoende och transparens är det inte ändamålsenligt att föreskriva om denna övervakning i en lag som gäller underrättelseverksamhet. Därför kommer det inom justitieministeriets förvaltningsområde att inrättas en ny myndighet för övervakning av underrättelseverksamheten. Även den parlamentariska övervakningen av underrättelseverksamheten kan anses tillhöra denna helhet.

Propositionen begränsar inte de högsta laglighetsövervakarnas verksamhet och den beräknas öka deras arbetsvolym. Detta påverkas dock av den lag om övervakning av underrättelseverksamheten som beretts vid justitieministeriet.

De bestämmelser om övervakning av användningen av underrättelseinhämtningsmetoder som föreslås i propositionen ökar såväl militärunderrättelsemyndighetens som försvarsministeriets rapporterings- och utredningsskyldigheter.

I Försvarsmaktens interna laglighetsövervakning strävar man efter att utnyttja den befintliga mekanismen för laglighetsövervakning, där laglighetsövervakningen utövas av huvudstabens juridiska avdelning som leds av Försvarsmaktens assessor. Den interna laglighetsövervakningen vid Försvarsmakten bör dock även kopplas samman med en komponent som utför teknisk övervakning. Vid Försvarsmaktens juridiska sektor saknas för närvarande de resurser och den kompetens som behövs för laglighetsövervakning som kräver tekniskt kunnande. För att trovärdigt kunna sköta sitt uppdrag behöver den interna laglighetsövervakningen vid Försvarsmakten två nya tjänster (1 jurist och 1 teknisk expert) som lyder under Försvarsmaktens assessor.

För laglighetsövervakningen vid försvarsministeriet behövs uppskattningsvis ytterligare ett årsverke på grund av de styrnings- och ledningsuppgifter som hänför sig till den nya verksamheten. Vid försvarsministeriet är det framför allt fråga om övervakningen och ordnandet av den interna laglighetsövervakningen inom Försvarsmakten.

Styrningen av den militära underrättelseverksamheten och samarbetet mellan den högsta statsledningen, statsrådet och de operativa aktörerna ökar arbetsvolymen vid försvarsministeriet.

Den föreslagna regleringen förtydligar fördelningen av behörighet mellan de säkerhetsmyndigheter som utför underrättelseinhämtning. Det skapas också en tydligare rättsgrund för det redan etablerade samarbetet.

Teleavlyssningen, teleövervakningen och inhämtandet av basstationsuppgifter ökar i viss mån antalet uppdrag för centralkriminalpolisen, eftersom den användning av befogenheter som behövs inom den militära underrättelseverksamheten ska genomföras med hjälp av de arrangemang som tillämpas för närvarande. Samtidigt kan användningen av hemliga metoder för informationsinhämtning anses minska något vid Försvarsmakten, vilket också minskar den informationsinhämtning som skyddspolisen utför åt Försvarsmakten.

Propositionen kan anses öka det internationella samarbetet vid Försvarsmakten, vilket förutsätter att resurser inriktas på detta.

Lagstiftningen om militär underrättelseverksamhet bidrar till att förbättra rättsskyddet för dem som deltar i underrättelseverksamheten. Dessutom ökar en tydlig och transparent lagstiftning rättssäkerheten och förbättrar det samhälleliga förtroendet i och med att aktörerna bättre kan bedöma den militära underrättelseverksamhetens effekter för samhället.

#### 4.1.4 Konsekvenser för hushållens ställning

Propositionen kan ha konsekvenser för hushållens beteende och det allmännas åtgärder kan ha ekonomiska konsekvenser även för hushållen. För det första har det i forskningslitteraturen förts fram att förändringar i förtroendet för sekretessen i fråga om meddelanden och internetanvändning kan påverka medborgarnas och konsumenternas beteende på ett sätt som kan ha ekonomiska och samhälleliga konsekvenser. Samtidigt har man genom att analysera konsumenternas praktiska val kunnat dra slutsatsen att integritetsskyddet kan ges en alltför stor betydelse i bedömningar som grundar sig på intervjuer. Konsumenternas intresse för bättre kryp-

tering av meddelanden och internettrafik kan växa om de upplever att integritetsskyddet försämras i övrigt.

Hushållen kan i och med den aktuella propositionen börja satsa mer på sin egen informationssäkerhet. Detta kan samtidigt förbättra hela samhällets skydd inte bara mot hot som avses i propositionen, utan även mot brottsrelaterade cyberhot.

En ökad användning av kommersiella informationssäkerhetslösningar kan även höja intresset för produkter från de företag som tillhandahåller dessa lösningar. Tillgången till kommersiella informationssäkerhetslösningar och köp av dem kan öka känslan av ojämlikhet mellan hushåll med olika utgångslägen.

Vad gäller kommunikationen på internet är det dessutom på grund av nätets funktionslogik redan nu möjligt för främmande staters myndigheter att utföra åtgärder som försvagar finländarnas integritetsskydd när de kommunicerar på internet, vilket konstaterats tidigare i motiveringen. Dessutom får kommersiella leverantörer av internettjänster med stöd av sina avtalsvillkor omfattande information om enskilda personer, vilket försvagar deras integritetsskydd.

Utifrån olika bedömningar kan man dock konstatera att finländarna är relativt väl medvetna om de försämringar av integritetsskyddet som gäller kommunikation på internet. Därmed kan det bedömas att de hushåll som är oroade över sin informationssäkerhet redan har beaktat att integritetsskyddet försämras i detta avseende.

På grund av både det som sagts ovan och den oberoende externa rättsliga och parlamentariska övervakningen kan konsekvenserna för hushållens ställning inte anses vara betydande.

### 4.2 Samhälleliga konsekvenser

#### 4.2.1 Medborgarnas ställning i samhället och verksamheten i det civila samhället

Förslaget har inga betydande konsekvenser för medborgarnas ställning i samhället, verksamheten i det civila samhället, medborgarnas värderingar och attityder, tillgodoseendet av de grundläggande rättigheterna och rättssäkerheten eller för samverkan och de juridiska förhållandena mellan medborgarna.

Förslaget bedöms inte ha några betydande konsekvenser för olika medborgargruppers ställning och beteende. Osäkerhet kring huruvida underrättelseinhämtningen inriktas rätt kan förebyggas genom att införa bestämmelser om principerna för militär underrättelseverksamhet och genom att underrättelseverksamheten ställs under oberoende rättslig och parlamentarisk övervakning.

Militärunderrättelsemyndighetens befogenheter möjliggör intrång i skyddet av konfidentiella meddelanden och integritetsskyddet. Den nya verksamheten kan till en början i vissa enskilda fall minska viljan för någon att använda sin yttrandefrihet och leda till självcensur i personens kommunikation. Konsekvenserna kan emellertid bedömas vara ytterst obetydliga. Samtidigt kan en oberoende och effektiv rättslig och parlamentarisk övervakning av den militära underrättelseverksamheten anses förebygga sådana konsekvenser.

Användningen av reservister för militär underrättelseverksamhet i vissa situationer ökar de värnpliktigas möjligheter att delta i Försvarsmaktens verksamhet. Försvarsmakten kan dra nytta av de värnpliktigas specialkompetens i större utsträckning än tidigare och detta kan an-

ses bidra till att öka försvarsviljan. Försvarsmakten kan utveckla värnplikten så att de värnpliktiga kan erbjudas utbildning som utvecklar deras specialkompetens. Med tanke på Försvarsmaktens eget behov innebär den föreslagna lagstiftningen att det uppstår nya arbetsuppgifter vid Försvarsmakten som kräver andra slags kompetenser och egenskaper än vad som behövs i den nuvarande verksamheten.

Propositionen bedöms inte påverka antalet repetitionsövningar eller värnplikten i normala situationer.

4.2.2 Konsekvenser för brottsbekämpningen och säkerheten

Förslaget ökar den mängd information som militärunderrättelsemyndigheten själv inhämtar och får av sina partner. Till den del informationen innehåller tecken på brott som anknyter till underrättelseverksamhet på det militära försvarets område eller till sådan verksamhet som äventyrar försvaret ansvarar Försvarsmakten precis som i dagsläget för förebyggandet och avslöjandet av dessa.

Vad gäller andra slag av brott ska militärunderrättelsemyndigheten utan dröjsmål underrätta förundersökningsmyndigheten om det medan en metod för underrättelseinhämtning används framgår att ett brott pågår, för vilket det strängaste föreskrivna straffet är fängelse i minst sex år, och brottet ännu kan förhindras. Militärunderrättelsemyndigheten får dessutom lämna sådan information till förundersökningsmyndigheten som syftar till att förhindra ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år.

I och med den föreslagna regleringen kan man i enskilda fall bättre förhindra att situationen utvecklas från förberedelse till genomförande av ett allvarligt brott. Det kan bedömas att det i samband med den militära underrättelseverksamheten varje år kommer fram högst ett grovt brott som leder till förundersökning och några allvarliga brott som ännu kan förhindras.

Regleringen om underrättelseinhämtningsmetoder skapar förutsättningar för inhämtning av information om verksamhet som utgör ett hot mot Finlands försvar eller allvarligt hotar den nationella säkerheten. Det är framför allt fråga om att skapa en lägesbild och ge information om utvecklingen i Finlands säkerhetspolitiska omgivning för landets högsta ledning och den högsta militära ledningen. Förslagen har ingen betydande allmän brottsförebyggande effekt, men i enskilda fall kan det bli möjligt att förhindra att en situation utvecklas så att ett allvarligt brott begås. Samtidigt kan bestämmelserna om underrättelseinhämtningsmetoder bidra till att höja tröskeln för att inleda brottslig verksamhet.

Dessutom kan information som inhämtats av militärunderrättelsemyndigheten användas för att rikta in Försvarsmaktens verksamhet, vilket förbättrar Försvarsmaktens förmåga att reagera på framväxande säkerhetshot och ger nya påverkansmöjligheter.

Förslaget möjliggör samarbete mellan den offentliga och den privata sektorn när det gäller att identifiera och bekämpa hot mot samhället och bevara den kritiska infrastrukturen och samhällets ekonomiska livskraft. Informationen ska utnyttjas t.ex. för att upprätthålla en gemensam nationell hotlägesbild. Enligt förslaget kan underrättelseinformation vid behov lämnas ut till privata sammanslutningar för att börja avvärja allvarliga hot eller förhindra avsevärda ekonomiska förluster.

Den militära underrättelsekapaciteten kan bedömas höja tröskeln för främmande stater att bedriva spionerier eller andra skadliga aktiviteter via datanäten mot Finland. Förslaget kan därmed

antas ha gynnsamma effekter på säkerheten i den digitala miljön i Finland, särskilt datasäkerheten och säkerheten i informationssystemen.

4.2.3 Konsekvenser för informationssamhället

Lagstiftningen om militär underrättelseverksamhet ser ut att få både direkta och indirekta konsekvenser för informationssamhället, framför allt till följd av de föreslagna nya befogenheterna till underrättelseinhämtning som avser datatrafik. De övriga befogenheter som föreslås i lagen om militär underrättelseverksamhet har mindre konsekvenser, eftersom de är digitala motsvarigheter till de hemliga metoder för informationsinhämtning som anges i 5 kap. i polislagen (teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, teknisk avlyssning).

Omfattningen av konsekvenserna för informationssamhället kan påverkas väsentlig genom lagstiftningstekniska lösningar. Vid valet av lösningsmodeller för lagstiftningen har man därför ända sedan lagstiftningsprojektet inleddes bedömt konsekvenserna av regleringen och beaktat den offentliga debatten.

Informations- och kommunikationsteknikens konsekvenser för företagens konkurrenskraft har samband med konsekvenserna för informationssamhället. Av dessa behandlas endast de direkta konsekvenserna i detta avsnitt.

4.2.3.1 Konsekvenser för användare av informationssamhällets tjänster

Med underrättelseinhämtning som avser datatrafik avses teknisk informationsinhämtning riktad mot datatrafik i kommunikationsnät som överskrider Finlands gräns, vilken baserar sig på automatiserad avskiljning av datatrafiken. Underrättelseinhämtning som avser datatrafik bedöms ha konsekvenser i fråga om utomstående personers rätt till konfidentiell kommunikation. Intrångets intensitet har begränsats genom lagstiftningstekniska val så att ingens rättigheter inskränks mer än vad som är nödvändigt för att utföra underrättelseinhämtning som avser datatrafik.

För det första ska denna typ av underrättelseinhämtning utföras vid en trafikknutpunkt. Tekniskt sett riktar sig traditionell teleavlyssning alltid mot en enskild teleadress (eller en begränsad grupp teleadresser). Då kan teleavlyssningen nättekniskt utföras nära den adress som är föremål för informationsinhämtning. Då kan det filter som används vid informationsinhämtningen ofta placeras vid en punkt i nätet som hanterar endast en liten mängd sådan trafik som inte omfattas av tillståndet för inhämtandet. En förutsättning för effektiv underrättelseinhämtning som avser datatrafik är att systemet för denna underrättelseinhämtning kan se en så stor del som möjligt av den datatrafik som är relevant för ändamålet med underrättelseinhämtningen. Detta kan åskådliggöras med ett exempel från den verkliga världen: om en myndighet får in ett tips om att en enskild speditionsfirma har långtradare som är i farligt dåligt skick, kan myndighetens informationsinhämtning riktas enbart mot denna speditionsfirmas terminal. Om myndigheten emellertid vill identifiera sådana långtradare i trafiken så effektivt som möjligt, måste observationen av trafikströmmarna koncentreras till knutpunkter i trafiken.

Eftersom underrättelseinhämtning som avser datatrafik sker i en punkt genom vilken en stor del av trafiken på nätet passerar, ska denna typ av underrättelseinhämtning inriktas enligt förhandsdefinierade strikta kriterier.

För det andra bör det noteras att nätet är oberoende av tid och plats. Även om underrättelseinhämtning som avser datatrafik endast används för datatrafik som överskrider riksgränserna kan även datatrafik inom landets gränser komma att omfattas av sökkriterierna på grund av sättet på vilket internet fungerar. Exempelvis vid hög belastning eller fel kan kontakten mellan två inhemska teleföretag ibland gå via en knutpunkt som finns utomlands. Överlag är det inte alltid tekniskt möjligt att direkt sluta sig till var en part som kommunicerar på internet befinner sig. Det är möjligt att det kommer fram att datatrafik som filtrerats för vidarebehandling är inhemsk först i samband med en manuell behandling som utförs av en underrättelseanalytiker. Därför ingår i förslaget ett särskilt förbud enligt vilket underrättelseinhämtning som avser datatrafik inte får riktas mot kommunikation där avsändaren och mottagaren befinner sig i Finland.

Av de föreslagna nya befogenheterna är det i synnerhet underrättelseinhämtning som avser datatrafik som kan öka medvetenheten om informationssäkerhetsrisker bland användarna av informationssamhällets tjänster och därmed öka deras användning av kommersiella informationssäkerhetslösningar.

4.2.3.2 Konsekvenser för informationssäkerheten och skyddet av den kritiska informationsinfrastrukturen

Underrättelseinhämtning som avser datatrafik bedöms ha en positiv inverkan på informationssäkerheten och på skyddet av den kritiska infrastrukturen.

Det är generellt sett mest effektivt att skyddet av information och observationer av avvikelser i informationssäkerheten sker så nära informationen som möjligt. Tidigare genomfördes skyddet i den organisation som äger informationen. Informationens betydelse som den viktigaste produktionsfaktorn i informationssamhället har dock ökat. Samtidigt har organisationernas förutsättningar att hantera riskerna mot deras eget informationskapital i viss mån försämrats till följd av de långa underleverantörskedjorna i samband med digitala tjänster. Informationens integritet, konfidentialitet och tillgänglighet är numera så väsentliga intressen som kräver skydd att hela samhället bör delta i skyddet av dem. Förutom informationssäkerhetsverksamhet i de organisationer som äger informationen och i företag som tillhandahåller IKT-tjänster och informationssäkerhetstjänster behövs effektivt fungerande myndigheter.

Underrättelseinhämtning som avser datatrafik förbättrar de behöriga myndigheternas förutsättningar att identifiera både cyberkartläggning av den kritiska infrastrukturen och statlig cyberspaning som riktas mot högteknologisk forsknings- och produktutvecklingsinformation. Det är till stor del privata företag som förvaltar den kritiska informationsinfrastrukturen och den högteknologiska produktutvecklingsinformationen i Finland. I syfte att förhindra skador har det därför i lagen om civil underrättelseinhämtning avseende datatrafik skapats förutsättningar för att lämna ut information som gäller hot mot informationssäkerheten till både kommunikationsverket och till företag som är föremål för en främmande stats informationsinhämtning. För att informationssäkerheten ska upprätthållas krävs samarbete mellan flera aktörer. Underrättelseinhämtning som avser datatrafik utgör en ytterligare komponent i detta samarbete.

Den eventuella ökningen av användningen av kommersiella informationssäkerhetslösningar som den föreslagna underrättelseinhämtningen medför bidrar till att öka den övergripande informationssäkerheten.

4.2.3.3 Konsekvenser för leverantörer av informationssamhällets tjänster

Av de befogenheter till informationsinhämtning som föreslås i 4 kap. i lagen om militär underrättelseverksamhet har teleavlyssning, inhämtande av information i stället för teleavlyssning och teleövervakning konsekvenser för leverantörer av informationssamhällets tjänster. Detta gäller åtminstone teleföretag, som är skyldiga att bistå myndigheterna med att genomföra kopplingar som behövs för användning av metoder för underrättelseinhämtning som avser teletrafik. De befogenheter som föreslås för militärunderrättelsemyndigheten ökar antalet aktörer som har rätt att använda dessa underrättelseinhämtningsmetoder. Det kan dock anses att konsekvenserna är neutrala jämfört med nuläget eller att de minskar företagens skyldigheter i viss mån. Teleavlyssning och teleövervakning ska inte längre användas för att inhämta information om brott utan för att identifiera vissa aktiviteter och hot. Tillstånd kan ges för högst sex månader åt gången. Förslaget om längre giltighetstid för tillstånd till inhämtande av information minskar belastningen på teleföretagens personalresurser vid långvariga operationer som gäller informationsinhämtning. Förslaget beräknas dessutom leda till en minskning av sådan informationsinhämtning som utförs av skyddspolisen inom ramen för Försvarsmaktens brottsbekämpning med de metoder som avses i detta kapitel.

Den nya typen av underrättelseinhämtning som avser datatrafik har en större inverkan på leverantörer av informationssamhällets tjänster, eftersom det för närvarande inte finns någon motsvarande lagstiftning. Underrättelseinhämtningen innebär att företag åläggs nya skyldigheter. Företagen föreslås få ersättning för de direkta kostnader, inklusive personalkostnader, som skyldigheterna medför.

Lagstiftningen ålägger inte företagen att bryta sina löften till kunderna i fråga om de mjukvaruprodukter eller informationssamhällstjänster som de tillhandahåller. Företagen behöver t.ex. inte överlåta krypteringsnycklar, installera bakdörrar eller införa begränsningar i användningen av kryptoprodukter.

4.2.3.4 Inriktning av underrättelseinhämtning som avser datatrafik på datatrafiken i ett kommunikationsnät

Det är svårt att få en exakt uppfattning av mängden datatrafik i ett kommunikationsnät. Mängden information i ett kommunikationsnät vid en given tidpunkt beror bl.a. på hur datatrafiken rör sig i andra delar av det globala kommunikationsnätet; t.ex. trafiken på internet styrs så att den kommer fram längs den väg som är effektivast.

Den mest exakta bilden av mängden datatrafik i en del av ett kommunikationsnät vid en given tidpunkt har den aktör som förvaltar den kommunikationsnätsdelen, i praktiken ägaren eller en aktör som t.ex. har hyrt en enskild fiber. Dessa uppgifter finns dock inte tillgängliga eftersom de omfattas av företagshemligheten.

Datatrafikmängderna kan dock uppskattas med hjälp av statistik som publiceras av aktörer som sköter internetknutpunkter (internet exchange, IX) i våra närområden. Endast en del av datatrafiken går genom de viktigaste knutpunkterna, men utifrån statistiken kan det uppskattas att mängden datatrafik till och från Finland uppgår till 1 terabit per sekund och mängden datatrafik som går genom Finland uppgår till 5–10 terabit per sekund, beroende på situationen.

Vid underrättelseinhämtning som avser datatrafik ska verksamheten inriktas på de kommunikationsnätsdelar som anges i domstolens tillstånd, såsom en enskild fiber, ett fiberpar eller en våglängd i en optisk kabel som går över Finlands gräns. I optiska kablar som går över Finlands gränser varierar antalet fiberpar i regel mellan färre än tio och upp till hundratals fiberpar. Med den våglängdsteknik som i dag används allmänt kan man i ett enda fiberpar förmedla

cirka 90 våglängder, dvs. kanaler. En enskild kanal har kapacitet för trafik på 100–400 gigabit per sekund beroende på vilken teknik som används och överföringsförbindelsens längd. Den maximala överföringskapaciteten för ett fiberpar varierar, men kan med den teknik som vanligen används i dag uppgå till 18 terabit per sekund vid internationella förbindelser. Den maximala överföringskapaciteten för en enskild optisk kabel beror på hur många fiberpar den innehåller.

Som tidigare konstaterats visar datatrafiken till, från och genom Finland att trafikmängderna är förhållandevis stora, även om underrättelseinhämtningen bara skulle fokusera på en våglängd. Exempelvis i fråga om datatrafik som skickas på en våglängd kan sådan trafik som är irrelevant för underrättelseinhämtningen ignoreras. Enligt bedömningar av de största företagen som utvecklar kommunikationsnätteknik var cirka 66 procent av all datatrafik år 2016 relaterad till videotjänster (t.ex. Netflix, HBO, Youtube) och musiktjänster (t.ex. Spotify). Enligt företagens bedömningar kommer 80 procent av all datatrafik år 2021 att bestå av videoöverföring.

Av datatrafiken kan dessutom uteslutas t.ex. den trafik som näthandeln ger upphov till. Enligt uppskattningar är dess andel cirka 6,5 procent av trafiken.

Efter att den trafik som beskrivs ovan har uteslutits omfattar underrättelseinhämtningen cirka 15 procent av den datatrafik som rör sig i den kommunikationsnätdel som domstolens tillstånd gäller, dvs. i praktiken 15 procent av datatrafiken på t.ex. en viss våglängd. De sökkriterier som avses i domstolens tillstånd inriktas på denna andel. Det kan uppskattas att cirka 0,5 procent av datatrafiken i den kommunikationsnätsdel som är föremål för underrättelseinhämtning filtreras från fall till fall för vidare behandling utifrån sökkriterierna.

Mängden relevant information som lagras i samband med den fortsatta behandlingen kan uppskattas uppgå till i genomsnitt 0,02 procent av den datatrafik som valts ut. Vilken mängd information som lagras beror framför allt på ändamålet med underrättelseinhämtningen. Till exempel ett videosamtal genererar datatrafik på mellan 300 kilobit per sekund och 5 megabit per sekund beroende på vilken bildkvalitet som används, dvs. en 1 minut lång videokonferens med bästa bildkvalitet motsvarar 300 000 kilobit, medan den aktuella propositionen i wordformat motsvarar cirka 4 240 kilobit.

Det är huvudsakligen stora organisationer som är föremål för militär underrättelseverksamhet. Organisationer kan antas ge upphov till mer omfattande datatrafik än enskilda personer. Därmed kan de sökkriterier som gäller organisationer antas ge effektivare resultat med avseende på det man vill få underrättelseinformation om. Således kan det antas att den datatrafik som lagras på basis av sökkriterier inte innehåller stora mängder onödig datatrafik.

I den föreslagna modellen för underrättelseinhämtning ska den datatrafik som filtrerats på basis av sökkriterier behandlas vidare, och ur den avlägsnas t.ex. information som är onödig på grund av skyldigheten att omedelbart förstöra data. Därmed är det endast en liten del av den datatrafik som motsvarar sökkriterierna som slutligen lagras. Av denna datatrafik lagras dessutom identifieringsuppgifter och andra uppgifter som gäller underrättelseuppdraget. Utifrån dessa kan man ytterligare inrikta den underrättelseinhämtning som avser datatrafik och den övriga underrättelseverksamheten. På behandlingen av personuppgifter tillämpas lagen om behandling av personuppgifter inom Försvarsmakten.

### 4.3 Jämförelse av för- och nackdelar

Acceptansen för den föreslagna lagstiftningen är delvis beroende av hur väl målen uppfylls och vilka konsekvenserna och kostnaderna för detta blir. Det viktiga är att man jämför de positiva och de negativa konsekvenserna av förslagen. Den nytta som underrättelseverksamheten medför för det militära försvaret och den nationella säkerheten måste vara större än den negativa inverkan som verksamheten eventuellt har på integritetsskyddet, samhällsekonomin och företagen. På grund av verksamhetens natur finns det t.ex. ingen offentlig information om hur stora ekonomiska resurser stater använder för militär underrättelseverksamhet.

#### 4.3.1 Avvärjande av hot mot det militära försvaret och den nationella säkerheten

Lagstiftningen om underrättelseverksamhet gör det möjligt att skapa en aktuell säkerhetslägesbild för myndigheterna samt föregripa och avvärja allvarliga hot som gäller det militära försvaret och den nationella säkerheten.

Regleringen om underrättelseinhämtningsmetoder skapar förutsättningar för inhämtning av information om militär verksamhet och verksamhet som utgör ett hot mot Finlands försvar eller allvarligt hotar den nationella säkerheten. Det är framför allt fråga om att inhämta tillförlitlig information i rätt tid till stöd för det säkerhetspolitiska och militära beslutsfattandet inom landets högsta ledning och den högsta militära ledningen för att de ska kunna skapa en lägesbild av utvecklingen i Finlands säkerhetspolitiska omgivning och av hoten i den. Propositionen stöder förutom försvaret även krishanteringsoperationer. Bristfällig underrättelseinformation om de områden där nuvarande och kommande krishanteringsoperationer utförs äventyrar säkerheten för finländare som delar i operationerna. De föreslagna befogenheterna ska också användas för att stödja andra myndigheter. Därför förbättrar propositionen också andra myndigheters förmåga att fullgöra sina lagstadgade uppgifter.

De hot som kan identifieras med hjälp av underrättelseinhämtning är internationella, allvarliga och riktar sig mot statens viktiga säkerhetsintressen. Underrättelseinhämtningen syftar till att ge ett skydd mot verksamhet som hotar den demokratiska stats- och samhällsordningen, de grundläggande samhällsfunktionerna, ett stort antal människors liv eller hälsa samt den internationella freden och säkerheten. Den största nyttan består i att sådana hot kan avvärjas.

Målet är att undanröja eller åtminstone minska de direkta och indirekta konsekvenserna av hoten. Direkta konsekvenser som genast kommer fram är t.ex. förlust av liv och hälsa eller materiella skador. Som exempel kan nämnas skadorna på regeringskvarteret i samband med terrorattacken i Norge i juli 2011, där de direkta kostnaderna för städning, reparation, anskaffning av tillfälliga lokaler och ökad säkerhetsövervakning har uppskattats till 1,45 miljarder norska kronor, vilket motsvarar cirka 150 miljoner euro (Minister Aasrud, Rigmor: intervju i Aftenposten).

Indirekta, fördröjda konsekvenser är exempelvis förluster för den internationella handeln, turismen och försäkringsbranschen, marknadsstörningar, skärpningar i kriminal- och säkerhetspolitiken och ökade utgifter i statsbudgeten. Till exempel utfördes en omfattande cyberattack mot Estland i samband med kontroversen kring den så kallade Bronssoldaten år 2007, vilket ledde till att flera bankers webbtjänster samt mediers och statliga myndigheters webbplatser kraschade. Även om det endast finns lite tillgänglig information om kostnaderna för attacken meddelade en estnisk bank att den hade orsakats ekonomiska skador på cirka 1 miljon amerikanska dollar (Herzog, Stephen: Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses).

4.3.2 Brottsbekämpning

I och med den föreslagna regleringen kan man i enskilda fall bättre förhindra att situationen utvecklas från förberedelse till genomförande av ett allvarligt brott. Det kan bedömas att det i samband med den militära underrättelseverksamheten varje år kommer fram högst ett grovt brott som leder till förundersökning och några allvarliga brott som ännu kan förhindras.

4.3.3 Tillgodoseende av de grundläggande fri- och rättigheterna

De bestämmelser som föreslås i propositionen innebär begränsningar av vissa grundläggande fri- och rättigheter, framför allt skyddet för privatlivet enligt grundlagens 10 § 1 mom., men även t.ex. rörelsefriheten, som tryggas i grundlagens 9 § 1 mom. Med tanke på de grundläggande fri- och rättigheterna är det fråga om en konkret nackdel som hänför sig till underrättelselagstiftningen, eftersom de föreslagna befogenheterna begränsar individens handlingsfrihet. I propositionen behandlas frågan om hur den militära underrättelseverksamheten kan ordnas så att den i så liten mån som möjligt begränsar integritetsskyddet och andra grundläggande fri- och rättigheter och är godtagbar med avseende på internationella människorättskonventioner. Det är svårt att bedöma nackdelarna, och man kan fråga sig om det alls är ändamålsenligt att försöka sätta ett ekonomiskt värde på t.ex. begränsningar av skyddet för privatlivet.

4.3.4 Direkta kostnadseffekter

Propositionen har konsekvenser för statsbudgeten. Den totala tilläggskostnaden för de nya myndighetsuppgifterna uppskattas i det inledande skedet till cirka 10 miljoner euro på årsnivå. Propositionen beräknas dessutom medföra ekonomiska konsekvenser på 3,4 miljoner euro för engångsanskaffningar under 2018. Under åren efter ikraftträdandeåret beräknas omkostnadsökningen uppgå till cirka 13,2–15,5 miljoner euro.

Den militära underrättelseverksamheten uppskattas orsaka övriga myndigheter årliga omkostnader på sammanlagt cirka 80 000 från och med det år då lagen föreslås träda i kraft.

4.3.5 Slutsatser

Eftersom de militära hoten mot Finland varierar till sin natur och under olika tider är det också svårt att förutse de direkta och indirekta kostnadseffekterna av hoten om de realiseras.

Om man bara lyckas avvärja ett enda hot kan besparingen i skadekostnader vara mångdubbel jämfört med de årliga omkostnaderna för den militära underrättelseverksamheten. Det kan därmed förväntas att fördelarna med förslaget överväger nackdelarna, inte bara i en jämförelse mellan skyddsintressen och begränsningar i handlingsfriheten som är svåra att värdera i pengar, utan också i ekonomiskt hänseende. Värdet på alla intressen som skyddas kan inte definieras i ekonomiska termer. I sista hand är det fråga om att upprätthålla den statliga suveräniteten.

## 5 Beredningen av propositionen

### 5.1 Beredningsskeden och beredningsmaterial

Den 1 oktober 2015 tillsatte försvarsministeriet en arbetsgrupp för att bereda ett förslag till lagstiftning om militär underrättelseinhämtning.

Projektet grundade sig på statsminister Juha Sipiläs regeringsprogram, där regeringen föreslår att underrättelseinhämtning som avser utländska förhållanden och underrättelseinhämtning som avser datatrafik ska basera sig på lagstiftning.

Arbetsgruppen hade till uppgift att bereda ett förslag till lagstiftning om bl.a. syftet med Försvarsmaktens underrättelseverksamhet, behöriga myndigheter och deras uppgifter och befogenheter samt styrning och övervakning, behandling och registrering av uppgifter och samarbete mellan myndigheterna. Det viktigaste målet med projektet var att förbättra den nationella säkerheten.

I arbetsgruppen ingick företrädare för försvarsministeriet, republikens presidents kansli, statsrådets kansli, utrikesministeriet, justitieministeriet, inrikesministeriet och huvudstaben. Till arbetsgruppen kallades också permanenta sakkunniga från Finlands näringsliv EK, Helsingfors universitet, utrikesministeriet, kommunikationsministeriet, skyddspolisen och Försvarsmakten.

I beslutet om att tillsätta arbetsgruppen konstateras det att beredningen av betänkandet bör ske med hänsyn till betänkandet från arbetsgruppen för en informationsinhämtningslag (Riktlinjer för en finsk underrättelselagstiftning. Betänkande av arbetsgruppen för en informationsinhämtningslag, 2015) och de remissyttranden som kom in om det.

Samtidigt tillsatte inrikesministeriet en arbetsgrupp för att bereda lagstiftning om civil underrättelseinhämtning och justitieministeriet en arbetsgrupp för att bereda lagstiftning om övervakningen av de civila och de militära myndigheternas underrättelseinhämtning. Dessutom utredde en sakkunnigarbetsgrupp som tillsatts av justitieministeriet en ändring av grundlagen så att det för att trygga den nationella säkerheten genom lag kan föreskrivas om begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden när de förutsättningar som ska anses behövliga uppfylls.

Arbetsgruppen överlämnade sitt betänkande till försvarsministeriet den 19 april 2017 (Förslag till lagstiftning om militär underrättelseverksamhet. Arbetsgruppsbetänkande, 2017; http://julkaisut.valtioneuvosto.fi/handle/10024/79757). Arbetsgruppen föreslog att en ny lag om militär underrättelseverksamhet ska stiftas.

Tillsättandet av den arbetsgrupp som beredde lagstiftningen om militär underrättelseverksamhet föregicks av en preliminär utredning. Försvarsministeriet tillsatte den 13 december 2013 en arbetsgrupp med uppgift att utveckla lagstiftning för att förbättra säkerhetsmyndigheternas förmåga att inhämta information om hot i cyberomgivningen. I arbetsgruppen för en informationsinhämtningslag ingick företrädare för försvarsministeriet, republikens presidents kansli, utrikesministeriet, justitieministeriet, inrikesministeriet, finansministeriet, kommunikationsministeriet, arbets- och näringsministeriet, Polisstyrelsen och huvudstaben. Till arbetsgruppen kallades dessutom permanenta sakkunniga.

Arbetsgruppens uppgift var att utveckla lagstiftning för att förbättra säkerhetsmyndigheternas förmåga att inhämta information om hot i cyberomgivningen och att bedöma behovet av att utveckla den finländska lagstiftningen så att man i Finland kan sörja för den nationella säkerheten genom att avvärja hot som förekommer i datanäten. Arbetsgruppen hade dessutom till uppgift att sammanställa synpunkter på säkerhetshot som riktas mot Finland via datanäten och hur de påverkar Finlands säkerhet och konkurrenskraft, att utreda nuläget vad gäller säkerhetsmyndigheternas informationsinhämtning och utvecklingsförslagen om den, att till behövliga delar undersöka vissa andra länders lagstiftning om säkerhetsmyndigheternas informat-

ionsinhämtning, att ta fram en konsekvensbedömning av de olika utvecklingsalternativen och mot bakgrund av detta komma med förslag till hur lagstiftningen ska utvecklas och vilka åtgärder genomförandet av dem förutsätter.

Arbetsgruppen överlämnade sitt betänkande till försvarsministeriet den 14 januari 2015 (Riktlinjer för en finsk underrättelselagstiftning. Betänkande av arbetsgruppen för en informationsanskaffningslag). Som bilagor till betänkandet ingick en avvikande åsikt och två yttranden. Arbetsgruppens betänkande var på omfattande remiss. Ett sammandrag av remissyttrandena har publicerats (Suomalaisen tiedustelulainsäädännön suuntaviivoja - lausuntoyhteenveto tiedonhankintalakityöryhmän mietinnöstä).

I betänkandet bedömdes behoven av att utveckla lagstiftningen om underrättelseverksamhet. Arbetsgruppen föreslog att regeringen bör överväga att inleda behövliga åtgärder för att skapa en rättsgrund för underrättelseverksamheten. De militära och civila myndigheter som ansvarar för den nationella säkerheten bör ges befogenheter att inhämta underrättelser om gränsöverskridande datatrafik för att vi ska kunna möta förändringarna i den säkerhetspolitiska omgivningen. Det är ändamålsenligt att koncentrera det tekniska utförandet av underrättelseinhämtning som avser datatrafik till en enda myndighet. Försvarsmakten och Skyddspolisen bör ges befogenheter att inhämta underrättelser som avser utländska förhållanden, så att underrättelseinhämtningen riktas mot personer och informationssystem. Underrättelseinhämtning som avser datatrafik bör förenas med ett oberoende tillståndsförfarande. Ett oberoende övervakningssystem bör skapas för underrättelseinhämtning som avser datatrafik och utländska förhållanden.

### 5.2 Remissyttranden och hur de har beaktats

Förslaget till lagstiftning om militär underrättelseverksamhet var på omfattande remiss. Begäran om utlåtande skickades till 119 instanser: riksdagspartier, myndigheter och andra aktörer. 72 remissinstanser yttrade sig. Begäran om utlåtande publicerades i elektronisk form i webbtjänsten utlåtande.fi och på försvarsministeriets webbplats. Ett sammandrag av yttrandena sammanställdes vid försvarsministeriet (Lagstiftning om militär underrättelseverksamhet, remissammandrag, 2017; http://urn.fi/URN:ISBN:978-951-25-2949-0). I sammandraget tas de kritiska synpunkterna i remissyttrandena upp.

Alla remissinstanser ansåg att lagstiftningen om militär underrättelseverksamhet behövs. Remissinstanserna kommenterade ett flertal mindre detaljer. Yttrandena har gåtts igenom noggrant och strävan har varit att i stor utsträckning beakta dem i regeringens proposition.

I avsnittet nedan behandlas centrala teman som har tagits upp i yttrandena.

#### 5.2.1 Ekonomiska konsekvenser

Remissinstanserna fäste uppmärksamhet vid de ekonomiska konsekvenser som presenterades i betänkandet, i synnerhet de ekonomiska konsekvenserna för åklagarväsendet och bedömningen av utgifterna för verkställighet av straff. I fråga om de ekonomiska konsekvenserna bör man också bedöma närmare hur brott som framkommer under underrättelseinhämtningen och överföringen av utredningsansvaret till polisen påverkar polisens arbete.

Remissinstanserna påpekade också att effektiviteten och kostnadseffektiviteten när det gäller underrättelseinhämtning som avser datatrafik bör bedömas närmare.

De ekonomiska konsekvenserna av regeringens proposition har kompletterats med uppgifter om justitieförvaltningens kostnader för eventuella brott som framkommer i samband med underrättelseverksamheten och för brott som ännu går att förhindra. Dessutom har tilläggskostnaderna för Försvarsmakten justerats.

5.2.2 Förhållande till grundlagen samt lagstiftningsordning

Remissinstanserna konstaterade att man i betänkandet har undervärderat den inskränkning av de grundläggande fri- och rättigheterna som de befogenheter som föreslås i betänkandet innebär. Till denna del önskade remissinstanserna att man vid den fortsatta beredningen fäster vikt vid hur de enskilda bestämmelser som är relevanta med tanke på grundlagen anses vara grundlagsenliga.

Avsnittet om förhållandet till grundlagen och lagstiftningsordningen har kompletterats under den fortsatta beredningen.

5.2.3 Föremål för den militära underrättelseinhämtningen

Remissinstanserna påpekade att föremålen för den militära underrättelseinhämtningen delvis överlappar motsvarande föremål som räknas upp i lagstiftningen om civil underrättelseverksamhet. I yttrandena fästes särskild uppmärksamhet på den punkt enligt vilken den militära underrättelseinhämtningen kan riktas mot verksamhet som hotar stats- och samhällsordningen.

Centralkriminalpolisen och polisstyrelsen konstaterade att föremålen för den militära underrättelseinhämtningen tangerar polisens verksamhetsfält i alltför hög grad. Dessutom påpekade myndigheter som använder hemliga informationsinhämtningsmetoder att det kan uppstå situationer där olika myndigheter som använder sådana metoder gör det inom samma område utan vetskap om varandra.

I den fortsatta beredningen har särskild uppmärksamhet ägnats åt föremålen för den militära underrättelseinhämtningen och åt samarbetet mellan olika myndigheter. Skillnaden mellan militär underrättelseinhämtning som gäller militär verksamhet och annan verksamhet har preciserats. Här har även regeringens proposition om ändring av grundlagen tagits i beaktande.

5.2.4 Utlämnande av uppgifter i vissa situationer

I yttrandena fästes särskild uppmärksamhet vid utlämnandet av information vid internationellt samarbete och till brottsbekämpningen. I fråga om brottsbekämpningen konstaterades det att betänkandets förslag om ett straffhot på två år innebär att ett stort antal brott skulle omfattas av militärunderrättelsemyndighetens anmälningsrätt.

Utifrån anmärkningarna i yttrandena har bestämmelserna om utlämnande av information harmoniserats med de motsvarande bestämmelser som föreslås i regeringens proposition om civil underrättelseinhämtning.

5.2.5 Förundersökning

Remissinstanserna påpekade att de tjänstemän som utför förundersökning och underrättelseverksamhet vid Försvarsmakten organisatoriskt sett bör åtskiljas från varandra tillräckligt tydligt. Under den fortsatta beredningen har propositionen kompletterats med ett förslag till lag

om ändring av lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Enligt förslaget ska denna skillnad inom organisationen förtydligas.

Enligt propositionen om civil underrättelseverksamhet ska skyddspolisens förundersökningsbefogenheter begränsas. Därför föreslås det att Centralkriminalpolisen i fortsättningen ska sörja för utredningen av sådana brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och sådana brott som äventyrar syftet med det militära försvaret.

5.2.6 Behandling av personuppgifter

I remissvaren fästes uppmärksamhet vid utlämnandet av information vid internationellt samarbete inom militär underrättelseverksamhet. För remissinstanserna var det oklart vilken typ av information som kan lämnas ut vid internationellt samarbete och enligt vilken bestämmelse i lagen; i betänkandet föreslogs att det i lagen också ska ingå bestämmelser om behandling av personuppgifter inom den militära underrättelseverksamheten.

Bestämmelserna om internationellt samarbete och motiveringarna till dem har preciserats utifrån yttrandena. Dessutom har bestämmelserna om utlämnande av information förtydligats genom att de bestämmelser om behandling av personuppgifter som föreslogs i betänkandet har flyttats till lagen om behandling av personuppgifter inom Försvarsmakten. Regeringen har för avsikt att lämna en proposition med förslag till lag om behandling av personuppgifter inom Försvarsmakten och till ändring av vissa lagar som har samband med den till riksdagen i februari 2018.

5.2.7 Utlåtande av rådet för bedömning av lagstiftningen

Ett utkast till regeringsproposition har behandlats av rådet för bedömning av lagstiftningen, som har gett ett utlåtande i frågan (http://vnk.fi/documents/10616/2913095/Lausunto+sotilastiedustelulaista+21.12.2017/f225ccef-4063-4515-a7e4-b34061f011c1). Rådet för bedömning av lagstiftningen anser att utkastet till proposition innehåller synnerligen omfattande beskrivningar av lagstiftningens nuläge, propositionens målsättningar, målgrupperna och de föreslagna åtgärderna. Viktiga verkningsområden och verkningsmekanismer för reformen har även identifierats och beskrivits, huvudsakligen ur ett kvalitativt perspektiv, i utkastet till proposition.

Bedömningsrådet har identifierat fem centrala utvecklingsobjekt. För det första bör konsekvenserna av lagen om militär underrättelseverksamhet klarare skiljas åt från underrättelselagarnas gemensamma konsekvenser.

För det andra bör en mera exakt bedömning göras av vilken verkan de nya befogenheterna har på Försvarsmaktens handlingsförmåga, t.ex. en effektivare verksamhet som en följd av den förbättrade förmågan till förvarning inom den militära underrättelseinhämtningen.

För det tredje bör det i propositionsutkastet presenteras en mera exakt kvalitativ beskrivning av fördelarna med de nya befogenheterna och av deras kostnadseffekter på strategisk, operativ och taktisk nivå för den militära underrättelseinhämtningen.

För det fjärde bör den internationella översikten i utkastet i den mån det är möjligt kompletteras med ett kortfattat sammandrag av läget i fråga om militär underrättelselagstiftning i de EU-länder som är viktigast för Finland. Till exempel en tabell som beskriver militärunderrättelse-

tjänsternas uppgifter och metoder för informationsinhämtning i olika länder skulle belysa saken betydligt.

För det femte bör en mera exakt uppskattning göras av de kostnader som företagen orsakas av militär underrättelseinhämtning och som staten ska ersätta.

Dessa iakttagelser av rådet för bedömning av lagstiftningen har beaktats i den fortsatta beredningen och på grund av utlåtandet har propositionen kompletterats till behövliga delar enligt rådets rekommendationer.

Det viktigaste målet med lagstiftningen om militär underrättelseverksamhet är att förbättra den nationella säkerheten och skapa en rättsgrund för underrättelseinhämtning. Projektet har nära samband med de lagstiftningsprojekt som gäller civil underrättelseverksamhet och övervakning av underrättelseverksamheten som är under beredning vid inrikesministeriet och justitieministeriet. Regeringen avser lämna propositioner om dessa till riksdagen samtidigt med den här propositionen. Lagförslagen syftar till att förbättra förutsättningarna för underrättelseinhämtning i Finland. I justitieministeriets proposition föreslås bestämmelser om extern laglighetsövervakning av den civila och den militära underrättelseverksamheten samt om vissa detaljer kring den parlamentariska övervakningen.

När projektet inleddes bedömde man olika lagstiftningstekniska lösningar och beslöt bl.a. av ändamålsenlighetsskäl att dela upp lagstiftningspaketet om underrättelseinhämtning i separata projekt som gäller civil underrättelseinhämtning, militär underrättelseinhämtning och ändring av grundlagen. Övervakningen av underrättelseverksamheten avskiljdes under beredningen till ett separat projekt. Lagförslagen i de separata propositionerna bildar också en helhet med avseende på bedömningen av konsekvenser. Konsekvensbedömningarna i propositionerna är dock individuella och gäller lagförslagen i respektive proposition. Exempelvis i justitieministeriets proposition gäller konsekvensbedömningarna de lagförslag som hänför sig till övervakning av underrättelseverksamheten. De ovannämnda lagförslagen kommer att behandlas samtidigt i riksdagen, vilket säkerställer att det finns en helhetsbild även med tanke på bedömningen av konsekvenserna.

På grund av den militära underrättelseverksamhetens natur kan bedömningen av konsekvenserna och kostnadseffekterna av eller fördelarna med de nya befogenheterna till underrättelseinhämtning inte beskrivas mer detaljerat i propositionen. Underrättelseinformation inhämtas för att man ska kunna förbereda sig på att hot realiseras. Det är inte alltid möjligt att entydigt avgöra vilka enskilda myndigheter eller samhällssektorer de ekonomiska konsekvenserna av underrättelseinformationen gäller. Beredskapen för hot är alltid beroende av när den genomförs; beredskapen påverkas av t.ex. den tekniska utvecklingen, de diplomatiska förbindelserna och hur de utvecklas samt av förändringar i samhället. De ekonomiska konsekvenserna för Försvarsmakten beror framför allt på att Försvarsmaktens verksamhet och de resurser som den har tillgång till kan inriktas och utökas i syfte att bemöta ett givet hot och sannolikheten för att det realiseras. Exempelvis kan underrättelseinformation om funktionerna i ett visst vapensystem styra Försvarsmaktens anskaffningar så att dessa funktioner beaktas på ett så effektivt sätt som möjligt. Information på strategisk nivå kan påverka Finlands utrikespolitiska relationer, medan information på taktisk och operativ nivå kan påverka innehållet i beväringsutbildningen. Samtidigt kan beredskap för t.ex. påverkan genom desinformation uppnås genom allmänna satsningar på utbildning och forskning.

Under den fortsatta beredningen har ett separat avsnitt om konsekvenser för hushållens ställning lagts till under rubriken Samhälleliga konsekvenser.

Verkställigheten av lagen och dess konsekvenser följs upp från och med ikraftträdandet. Syftet med uppföljningen är att bedöma hur lagen fungerar och eventuella ändringsbehov i den. Den information som samlas in vid uppföljningen behövs på längre sikt även som grund för kommande lagstiftningsreformer.

Det handlar om en helt ny lagstiftningshelhet vars konsekvenser bör bedömas både på förhand och i synnerhet i efterhand. Därför kan det föreslås att riksdagen bör överväga att förena godkännandet med en skyldighet att följa upp verkställigheten av lagstiftningen. Det är ändamålsenligt att uppföljningsperioden är tillräckligt lång för att det ska finnas tillräckligt med material för efterhandsbedömningen. När indikatorerna för uppföljningen utses är de viktigt att de bildar en helhet som kan ge så omfattande och objektiv information som möjligt för att man ska kunna dra behövliga slutsatser. I efterhandsbedömningen bör särskild hänsyn tas till att utrikespolitiskt och på andra sätt känsliga frågor som hänger samman med underrättelseverksamheten kan ställa vissa begränsningar för valet av uppföljningsindikatorer.

Bedömningsrådets förslag om en tabell som beskriver militärunderrättelsetjänsternas uppgifter och metoder för informationsinhämtning i de viktigaste EU-länderna ansågs inte nödvändigt att genomföra, eftersom tabellen skulle bli ytterst omfattande och inte en ge tydligare bild av helheten. De lagstiftningsmässiga lösningarna i olika länder avviker betydligt från varandra t.ex. vad gäller avgränsningen, och en jämförelse av dem skulle inte tillföra något mervärde för konsekvensbedömningen. Till avsnittet om den internationella utvecklingen och lagstiftningen i utlandet och i EU har dock fogats en redogörelse för på vilka grunder de länder som behandlas har valts ut.

De kostnader som användningen av befogenheterna orsakar företagen har bedömts så exakt som det var möjligt när propositionen utarbetades. Kostnaderna för företagen beror framför allt på hur den tillståndspraxis som användningen av befogenheterna förutsätter kommer att utvecklas. Dessutom påverkas kostnaderna av vilka system som behövs för användningen av befogenheterna. Enligt den ersättningspraxis som ska fortsätta gälla får företagen ersättning endast för kostnader för utveckling av systemen, inte för arbetskraft, vilket kan ha väckt farhågor om att underrättelsemyndigheterna inte vill utveckla system som kräver mindre personalresurser. Detta anses dock inte vara ändamålsenligt med tanke på myndighetsverksamheten. Tvärtemot är det ändamålsenligt att utveckla ett system som kräver mindre personal, särskilt på grund av den nya verksamhetens känsliga natur. Det är också ändamålsenligt med tanke på verksamhetens natur att myndigheterna strävar efter att sköta de behövliga åtgärderna i egen regi så långt det är möjligt.

I fråga om underrättelseinhämtning som avser datatrafik bör det dock noteras att företagens direkta kostnader ska ersättas.

## 6 Ålands ställning

Enligt grundlagens 120 § har landskapet Åland självstyrelse enligt vad som särskilt bestäms i självstyrelselagen för Åland. I självstyrelselagen för Åland (1144/1991) föreskrivs bl.a. om åländsk hembygdsrätt, fördelningen av lagstiftningsbehörigheten mellan riket och landskapet, lagstiftningskontrollen, förvaltningsbehörigheten, rättskipningen, språk- och kulturärenden samt om landskapets ekonomi.

Lagtinget är det åländska parlamentet i fråga om självstyrelsen. Landskapets förvaltning sköts av Ålands landskapsregering och myndigheterna under denna. Länsstyrelsen för landskapet Åland och myndigheterna vid statens ämbetshus i Mariehamn sköter de uppgifter som hör till

riksmyndigheternas allmänna förvaltning på Åland. Ålandsdelegationen är ett gemensamt organ för landskapet och riket som sköter vissa i självstyrelselagen angivna uppgifter. Delegationen ska bl.a. sköta sakkunniguppgifter som gäller självstyrelsen och avge utlåtanden till statsrådet och ministerierna.

Åland har varit ett demilitariserat område sedan 1856 efter Krimkriget. Sedan dess har väpnade styrkor endast befunnit sig där under världskrigen. Ålands demilitarisering fastställdes genom 1922 års konvention angående Ålandsöarnas icke-befästande och neutralisering (FördrS 1/1922) mellan Finland, Tyskland, Danmark, Sverige, Brittiska riket, Frankrike, Italien, Lettland och Polen. Därtill har Finland och Sovjetunionen slutit ett särskilt fördrag om Ålandsöarnas demilitarisering 1940 (FördrS 24/1940). De båda överenskommelserna förbjuder Finland att uppföra några som helst fasta försvarsanläggningar, militärflygplatser eller andra anordningar avsedda för militära ändamål. I händelse av krig har Finland enligt 1922 års konvention rätt att minera åländska vatten och placera ut trupper på Ålands territorium för att avvärja anfall som hotar dess neutralisering. Den grundläggande principen är dock att signatärstaterna ska låta Åland stå utanför krigshandlingar även i krigssituationer.

De ovannämnda överenskommelserna om Åland definierar bl.a. vilka rättigheter och skyldigheter Finlands försvarsmakt har på Ålands territorium. I artikel 4 i konventionen angående Ålandsöarnas icke-befästande och neutralisering (1922) bestäms om rätten för fartyg att besöka öarna. Enligt artikel 7 är Finland skyldigt att övervaka den åländska zonen och ha beredskap att försvara den. Med den åländska zonen avses det område som definieras i 1922 års konvention angående Ålandsöarnas icke-befästande och neutralisering och 1940 års fördrag mellan Finland och de Socialistiska Sovjetrepublikernas Förbund angående Ålandsöarna.

Marinen har rätt att tidvis inspektera öarna med högst två krigsfartyg (artikel 4.2 b i konventionen). I praktiken har Ålands landskapsregering underrättats på förhand om dessa inspektioner och besök. Besöken planeras på förhand. Högst två av marinens fartyg får befinna sig samtidigt på landskapet Ålands territorium. Ett enskilt inspektionsbesök får vara högst 48 timmar långt. Tidsbegränsningen gäller inte avvärjande av territorieförseelser eller handräckningsuppgifter. Kommendören för marinen fastställer den årliga planen för marinens inspektionsbesök och beviljar tillstånd för de finländska krigsfartygens besök och genomfart till den åländska zonen. Situationsenliga besök som avviker från den på förhand upprättade inspektionsplanen behandlas separat.

Lagstiftningsmakten i ärenden som gäller det åländska självstyret tillkommer landskapet. I 27 § och 29 § självstyrelselagen för Åland anges på vilka områden rikets lagstiftning även gäller på Åland. I självstyrelselagen anges dels på vilka områden landskapet har behörighet att lagstifta och dels på vilka områden riket har behörighet att lagstifta. Rättsskipningen inom landskapet hör i allmänhet till uppgiftsområdet för det vederbörande statliga organet. Domsrätten brukas således av rikets domstolar eller andra riksmyndigheter som blivit beviljade lagskipningsmakt. Detsamma gäller även den förvaltningsrättsliga lagskipningen.

Enligt 27 § 34 punkten i självstyrelselagen för Åland har riket lagstiftningsbehörighet i fråga om försvarsväsendet och gränsbevakningen med beaktande av vad som föreskrivs i 12 §, ordningsmaktens verksamhet för tryggande av statens säkerhet, försvarstillstånd, beredskap inför undantagsförhållanden. Lagförslaget hör därmed till rikets lagstiftningsbehörighet. Förslaget påverkar inte Ålands ställning eller de internationella överenskommelser som Ålands neutralitet och demilitariserade status grundar sig på.

## 7 Samband med andra propositioner

Propositionen har ett direkt samband med de propositioner med förslag till lagar om civil underrättelseinhämtning och övervakning av underrättelseverksamheten som beretts vid inrikesministeriet och justitieministeriet.

Dessutom har propositionen samband med en proposition som beretts vid justitieministeriet. I den föreslås att en ny bestämmelse om begränsning av skyddet för hemligheten i fråga om förtroliga meddelanden ska införas i grundlagen. Ändringen gör det möjligt att införa lagstiftning om befogenheter till underrättelseinhämtning som begränsar skyddet för hemligheten i fråga om förtroliga meddelanden.

I 2 § i det förslag till lag om militär underrättelseverksamhet som ingår i propositionen finns en hänvisningsbestämmelse till det nya 5 a kap. i polislagen som gäller civil underrättelseinhämtning, till lagen om civil underrättelseinhämtning avseende datatrafik och till lagen om övervakning av underrättelseverksamheten. Enligt 70 § 2 mom. i det ovannämnda lagförslaget finns bestämmelser om det tekniska genomförandet av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning i 10 § i lagen om civil underrättelseinhämtning avseende datatrafik.

Behandlingen av alla ovannämnda propositioner bör samordnas i riksdagen.

Propositionen har ett nära samband med den ändring av riksdagens arbetsordning som är under beredning i riksdagen och som syftar till att organisera den parlamentariska övervakningen av underrättelseverksamheten. Ändringen av riksdagens arbetsordning kommer att göras genom talmanskonferensens förslag.

Propositionen anknyter också till en proposition med förslag till en ny lag om behandling av personuppgifter inom Försvarsmakten som har beretts vid försvarsministeriet. I lagen samlas bestämmelser om behandling av personuppgifter inom Försvarsmakten. I lagen tas dessutom in en helt ny helhet som gäller behandling av personuppgifter med anknytning till militär underrättelseverksamhet. Propositionen har samband med totalreformen av den finska dataskyddslagstiftningen som bygger på EU:s dataskyddspaket. De lagförslag som ingår i propositionen avses träda i kraft den 6 maj 2018.

## DETALJMOTIVERING

### 1 Lagförslag

### 1.1 Lagen om militär underrättelseverksamhet

1 kap. Allmänna bestämmelser

**1 §.** *Tillämpningsområde.* I paragrafen föreskrivs det om lagens tillämpningsområde. Den underrättelseinhämtning som avses i denna lag utförs av Försvarsmakten och kallas för militär underrättelseinhämtning. Målet med underrättelseverksamheten är att i ett tidigt skede inhämta sådan information i anslutning till Försvarsmaktens uppgifter som möjliggör att man har beredskap för och kan påverka hot, risker, eventuella händelseförlopp och förändringar. Den militära underrättelseinhämtningens allmänna uppgift är att skapa en militärstrategisk lägesbild genom att följa utvecklingen i Finlands säkerhetspolitiska miljö, fastställa förändringar i den och producera information om det rådande läget. I lagen föreskrivs det om syftet med den militära underrättelseinhämtningen, om myndigheternas uppgifter och befogenheter, om beslutsfattande samt om styrningen av den militära underrättelseinhämtningen och övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen. Lagen innehåller också bestämmelser om det tekniska genomförandet av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning.

**2 §.** *Förhållande till annan lagstiftning.* I 1 mom. föreskrivs det om lagens förhållande till annan verksamhet som har nära samband med militär underrättelseverksamhet.

I regeringens proposition till riksdagen med förslag till lag om ändring av polislagen (RP /2017) föreslås att det till polislagen ska fogas ett nytt 5 a kap. enligt vilket skyddspolisen sköter uppgifter som gäller civil underrättelseinhämtning.

Enligt RP /2017 ska det i 5 a kap. fastställas att tillämpningsområdet för metoderna för underrättelseinhämtning är den underrättelseinhämtning som utförs av skyddspolisen och som används för att inhämta information om verksamhet som allvarligt hotar den nationella säkerheten. Genom regleringen betonas det att skyddspolisen är den enda civila underrättelsemyndighet som har rätt att använda de metoder som avses i 5 a kap. i polislagen.

I tillämpningsområdet för 5 a kap. ska det enligt RP /2017 finnas en hänvisning till lagen om civil underrättelseinhämtning avseende datatrafik. En befogenhet inom civil underrättelseinhämtning är enligt 5 a kap. informationsinhämtning som avses i en särskild lag och riktas mot den datatrafik som rör sig i de telekommunikationskablar som överskrider den finska gränsen.

Det tekniska genomförandet av inhämtande av information om datatrafik som rör sig i de telekommunikationskablar som överskrider den finska gränsen är koncentrerat till en aktör inom Försvarsmakten som är skyldig att fullgöra de uppdrag som skyddspolisen ger den och som gäller denna metod för inhämtande av information. Bestämmelser om vem som ansvarar för det tekniska genomförandet ska finnas i lagen om militär underrättelseverksamhet.

Militär underrättelseinhämtning ska enligt 2 mom. åtskiljas från Försvarsmaktens förebyggande, avslöjande och utredning av brott som det finns bestämmelser om i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014). Enligt 86 § 1 mom. i den lagen sörjs det vid försvarsmaktens förebyggande och avslöjande av brott för att brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets om-

råde och till sådan verksamhet som äventyrar syftet med det militära försvaret förebyggs och avslöjas. I 89 § 2 mom. i samma lag fastställs det vid avslöjandet av vilka brott hemliga metoder för inhämtande av information får användas. Tillämpningsområdet för den brottsbekämpning som avses i lagen om militär disciplin och brottsbekämpning inom försvarsmakten har samband med begreppet brott och detta begrepp ska skiljas från hot och verksamhet som är föremål för underrättelseinhämtning samt utvecklingen av dessa hot och denna verksamhet. Befogenheterna enligt den lagen utövas av Huvudstabens underrättelseavdelning. Eftersom befogenheterna till brottsbekämpning delvis är likadana som de befogenheter som föreslås i denna proposition, men utövas för olika syften, ska särskild uppmärksamhet fästas vid att befogenheterna till militär underrättelseinhämtning och befogenheterna till brottsbekämpning inte utövas av samma personer.

I denna regeringsproposition föreslås det också att lagen om militär disciplin och brottsbekämpning inom försvarsmakten ska ändras så att man skiljer på personer som utövar befogenheter till underrättelseinhämtning och personer som utövar befogenheter till brottsbekämpning. Dessutom ska den myndighet som utför förundersökning av brott enligt den lagen ändras i och med att skyddspolisen avstår från sina befogenheter till förundersökning.

I 3 mom. föreskrivs det om tillämpningen av lagen om behandling av personuppgifter inom Försvarsmakten. En hänvisningsbestämmelse har ansetts behövlig eftersom Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) ska tillämpas på behandlingen av personuppgifter om det inte finns en särskild hänvisningsbestämmelse. En informativ hänvisning till allmänna lagar, såsom lagen om offentlighet i myndigheternas verksamhet (621/1999), har inte ansetts vara behövlig.

På grund av underrättelseverksamhetens art ska särskild uppmärksamhet ägnas åt övervakningen av denna verksamhet. I Europadomstolens avgörandepraxis har det betonats att övervakningen ska vara oberoende och inte höra till underrättelsemyndighetens förvaltningsområde. Den rättsliga övervakning som står utanför underrättelseverksamheten ska vara koncentrerad till underrättelseombudsmannen, som det föreskrivs särskilt om.

**3 §.** *Syftet med den militära underrättelseinhämtningen.* I paragrafen definieras syftet med den militära underrättelseinhämtningen. Enligt 1 mom. är syftet med den militära underrättelseinhämtningen begränsat så att det gäller vissa av Försvarsmaktens lagstadgade uppgifter samt stödjande av den högsta statsledningens beslutsfattande. Paragrafen har en genomgripande betydelse för hela lagen. Med stöd av paragrafen kan det också bedömas om underrättelseinhämtning om en viss verksamhet hör till den militära eller den civila underrättelseinhämtningens ansvarsområde. Den militära underrättelseinhämtningen och metoderna för underrättelseinhämtning ska möjliggöra att militärunderrättelsemyndigheten tillräckligt effektivt kan inhämta information om de företeelser och verksamheter som mest hotar samhället och dess existens.

Försvarsmaktens uppgifter omfattar i stor utsträckning också den högsta statsledningens beslutsfattande och att informera den högsta statsledningen om förändringar i den säkerhetspolitiska omgivningen. Dessutom förutsätter t.ex. beslutsfattandet om och prövningen av Försvarsmaktens internationella uppdrag alltid beslutsfattande av den högsta statsledningen. Trots att den högsta statsledningens beslutsfattande utgör en väsentlig del av Försvarsmaktens verksamhet ska stödjande av den högsta statsledningens beslutsfattande nämnas särskilt i paragrafen. Omnämnandet är informativt.

I det förslag som är under behandling föreslås dessutom att det nedan ska föreskrivas om styrningen av den militära underrättelseinhämtningen. En central del av denna styrning utgörs av det gemensamma mötet mellan statsrådets utrikes- och säkerhetspolitiska ministerutskott och republikens president samt den begäran om information som endast vissa utrikes- och säkerhetspolitiskt betydelsefulla finska aktörer kan lämna till militärunderrättelsemyndigheten. Av de orsaker som beskrivs ovan är det inte ändamålsenligt att den högsta statsledningen i Finland nämns särskilt eftersom den högsta statsledningen är en viktig mottagare av underrättelseinformation.

De åtgärder som vidtas på basis av den information som inhämtats och analyserats kan vara av många slag. Åtgärderna kan inbegripa t.ex. förbättring av lägesuppfattningen hos människor som befinner sig på finskt territorium och satsningar på utbildning, såsom vid desinformationsoperationer, samt i extremfall mobilisering. I det första exemplet lämnar den högsta statsledningen underrättelseinformationen till de behöriga myndigheterna. Det är dock inte i alla situationer nödvändigtvis statsledningen som sprider informationen vidare till de behövliga aktörerna, utan i fall där t.ex. avancerade sabotageprogram identifierats kan information om ett sabotageprogram lämnas direkt till de berörda företagen för att säkerställa att statsledningens beslutsfattande tryggas.

Syftet med den militära underrättelseinhämtningen är enligt paragrafen bundet till vissa av Försvarsmaktens uppgifter som avses i lagen om försvarsmakten. Enligt 2 § 1 mom. 1 punkten i lagen om försvarsmakten hör det militära försvaret av Finland till försvarsmaktens uppgifter. Det militära försvaret av Finland innefattar enligt 1 punkten underpunkt a övervakning av landområdena, vattenområdena och luftrummet samt tryggande av den territoriella integriteten. Enligt 1 punkten underpunkt b innefattar det militära försvaret av Finland också tryggande av befolkningens livsbetingelser, de grundläggande fri- och rättigheterna och statsledningens handlingsfrihet samt försvar av den lagliga samhällsordningen.

Försvarsmaktens första lagstadgade uppgift har ansetts innebära att Försvarsmakten ska skydda Finland mot yttre hot. Ett yttre hot inbegriper dock inte nödvändigtvis sådan verksamhet utanför Finlands gränser som riktar sig mot Finland, utan strävan kan också vara att ett hot ska förverkligas på finskt territorium. En utländsk aktör kan försöka förbereda och organisera militär verksamhet med hjälp av t.ex. personer som befinner sig i Finland.

Genom militär underrättelseinhämtning försöker man reda ut vilka aktörer som ligger bakom denna typ av hot och hur de försöker påverka Finland och t.ex. Finlands militära försvar. Verksamhet som sker i Finland kan också syfta till att påverka de krishanteringsinsatser som Finland deltar i eller utgöra hybridpåverkan i Finland. Av betydelse är att en främmande stat eller utländsk aktör ligger bakom verksamheten.

Till försvarsmaktens uppgifter hör enligt 2 § 1 mom. 3 punkten i lagen om försvarsmakten också deltagande i stöd och bistånd som grundar sig på artikel 222 i fördraget om Europeiska unionens funktionssätt eller artikel 42.7 i fördraget om Europeiska unionen samt deltagande i territorialövervakningssamarbete eller i annat internationellt bistånd och annan internationell verksamhet.

I enlighet med 2 § 1 mom. 3 punkten i lagen om försvarsmakten ska Finlands militära försvar stärkas genom internationellt samarbete. Samarbete idkas inom EU och med andra stater och internationella organisationer, såsom FN och Nato, samt med olika grupper av länder. Internationellt bistånd kan i enlighet med 3 punkten ges en annan stat, Europeiska unionen eller en internationell organisation t.ex. i situationer som inkluderar EU:s solidaritetsklausul eller klau-

sul om ömsesidigt bistånd eller vid territorialövervakning på det sätt som föreskrivs i lagen om försvarsmakten. Som exempel på annan internationell verksamhet som avses i bestämmelsen kan nämnas samverkan som utgår från Finlands egna behov.

Enligt 2 § 1 mom. 4 punkten i lagen om försvarsmakten hör till försvarsmaktens uppgifter också deltagande i internationell militär krishantering och i militära uppdrag i annan internationell krishantering.

Det kan utöver vad som föreskrivs ovan dessutom också bli aktuellt att indirekt stödja andra myndigheter. Som en sådan särskild situation kan betraktas den handräckning som Försvarsmakten ger polisen. Trots att stödjande av andra myndigheter inte nämns i paragrafen kan militär underrättelseinhämtning indirekt bli aktuell i situationer där handräckning ges. Om t.ex. polisen begär handräckning av Försvarsmakten utomlands kan man bli tvungen att använda militär underrättelseinhämtning för endast försvarsmaktens egen verksamhet. Det är i detta fall inte fråga om underrättelseverksamhet som utförs för polisens räkning. Underrättelseinformationen stöder Försvarsmaktens verksamhet och lämnas i dessa fall inte ut till polisen.

Syftet med den militära underrättelseinhämtningen är att i ett tillräckligt tidigt skede inhämta korrekt och oberoende information till stöd för den högsta militära ledningens beslutsfattande avseende de av Försvarsmaktens uppgifter som anges i 2 § i lagen om försvarsmakten samt i sista hand till stöd för den högsta statsledningens beslutsfattande. Information får inhämtas endast om de föremål för militär underrättelseinhämtning som anges i denna lag. Den information som inhämtats genom militär underrättelseinhämtning möjliggör att den högsta militära ledningen och den högsta statsledningen i rättidigt kan fatta beslut som grundar sig på korrekt information och att en strategisk, operativ och taktisk förvarning kan ges. Informationen möjliggör också att de tillgängliga myndighetsresurserna används effektivt och att myndighetsresurserna planeras, utvecklas, upprätthålls och utökas effektivt i tillräckligt god tid, om situationen kräver det.

Inhämtandet av information inbegriper också kartläggning av yttre hot som riktar sig mot Finland. Det är alltså fråga om att t.ex. följa upp utvecklingen av den säkerhetspolitiska miljön för att kunna skapa en lägesbild. Begreppet inhämtande av information täcker också fortgående inhämtande av information om föremål för militär underrättelseinhämtning. Inhämtandet av information kan inte i sig begränsas tidsmässigt eftersom underrättelseverksamhet ofta måste pågå under en lång tid och vara systematisk, utan att den verksamhet som är föremål för underrättelseinhämtning nödvändigtvis behöver utgöra en överhängande fara under den tid underrättelseinhämtningen pågår. Till denna del kan det hänvisas till justitieministeriets betänkande om en ändring av grundlagen (justitieministeriets betänkanden och utlåtanden 41/2016 s. 49).

Händelseförlopp och verksamheter kan till en början verka vara något annat än verksamhet som utgör ett konkret hot. Att man i ett tillräckligt tidigt skede får information om dessa händelser och denna verksamhet möjliggör att man kan identifiera målet med dem och reda ut vem som har intresse och nytta av dem. Detta möjliggör också att det kan göras en tillräcklig riskbedömning och utrikes-, säkerhets- och försvarspolitisk bedömning av hur sannolikt det är att Finland blir och i vilka situationer Finland kan bli föremål för denna typ av händelseförlopp och verksamhet. Vid identifieringen av hot är det viktigt att reda ut vilken aktör som ligger bakom hotet och med vilka resurser hotet kan förverkligas.

Ett viktigt föremål för militär underrättelseinhämtning är t.ex. militär verksamhet. Militär verksamhet kan vara ett yttre hot mot Finland som en statlig eller icke-statlig aktör ligger

bakom (justitieministeriets betänkanden och utlåtanden 41/2016 s. 48). I samband med militär verksamhet förflyttas ofta stora truppenheter och vapensystem. Placeringen av truppenheter och vapensystem ger information om den militära aktörens insatsberedskap under fredstid t.ex. vid militära övningar.

Underrättelseinhämtning om hot täcker också t.ex. framtagning av det målidentifieringsstöd och de geografiska uppgifter och uppgifter om förhållanden som Försvarsmakten behöver.

Syftet med den militära underrättelseinhämtningens inhämtande av information är inte att påverka själva verksamheten utan att inhämta information om den och de avsikter och drivfjädrar som ligger bakom den. En verksamhet kan t.ex. vara helt normal, men organiseringen av den kan ha sitt ursprung i en främmande stats försök att påverka verksamheten i ett demokratiskt samhälle. I sådana situationer är det mycket viktigt att inhämta information om huruvida en främmande stat utövar inflytande över ledarna för en intern konflikt eller styr den eller om en främmande stat själv bör ansvara för denna typ av verksamhet. Verksamheten kan utgöra ett led i en främmande stats krigsplaner eller en första fas i en främmande stats användning av militära maktmedel.

Syftet med den militära underrättelseinhämtningen är inte att ingripa i t.ex. sådan privat verksamhet av internationell karaktär som kan anses vara helt normal, såsom konkurrens på marknadsvillkor eller lagliga rättsprocesser och immaterialrättigheter. Föremål för underrättelseinhämtning kan också i dessa fall bli de faktorer som ligger bakom verksamheten, såsom en främmande stats beslut att förbjuda export till Finland av en produkt eller råvara som är livsviktig för Finland och som produceras av bolag som den främmande staten äger och att på detta sätt försöka påverka den fria verksamheten i det finländska samhället. Också i dessa situationer behöver Försvarsmakten inte nödvändigtvis vidta konkreta åtgärder utifrån den erhållna informationen, utan informationen om de faktorer som ligger bakom verksamheten kan om ett hot är tillräckligt allvarligt lämnas till de centrala aktörer som kan vidta behövliga åtgärder för att begränsa hotets konsekvenser och rätta till situationen.

Paragrafens betydelse framgår också av det faktum att vid militär underrättelseverksamhet syftar inhämtandet av information alltid till att genomföra vissa av de uppgifter som Försvarsmakten har enligt lagen om försvarsmakten. De nedan angivna föremålen för den militära underrättelseinhämtningen ska alltid basera sig på syftet med den militära underrättelseinhämtningen, och de metoder för underrättelseinhämtning som avses i 4 kap. kan användas endast för Försvarsmaktens uppgifter som räknas upp i den föreslagna paragrafen och utförande av ett underrättelseuppdrag som baserar sig på föremålen för den militära underrättelseinhämtningen.

**4 §.** *Föremål för den militära underrättelseinhämtningen.* I paragrafen föreskrivs det om vilken verksamhet som information kan inhämtas om med den militära underrättelseinhämtningens metoder för underrättelseinhämtning. Bestämmelser om metoder för underrättelseinhämtning finns i 4 kap. Genom militär underrättelseinhämtning inhämtas alltid den information som behövs för att genomföra Försvarsmaktens lagstadgade uppgifter enligt 3 §. Paragrafen har betydelse för den som framställer en begäran om information, den som delar ut ett underrättelseuppdrag och den som framför ett yrkande på att en metod för underrättelseinhämtning ska användas samt den aktör som fattar beslut på basis av yrkandet eller den som beviljar tillstånd. Beslutsfattarens prövning av respektive fall omfattar huruvida t.ex. underrättelseinhämtning som avser datatrafik kan användas för att inhämta information om en främmande stats verksamhet som kan äventyra det finska försvaret.

I paragrafen anges det ingen geografisk begränsning för var den verksamhet som underrättelseinhämtningen gäller ska ske. Det är inte ändamålsenligt att en underrättelseoperation inleds utanför Finlands gränser och att operationen måste avbrytas när den aktör som är föremål för underrättelseinhämtning anländer till Finland.

Verksamhet som är föremål för militär underrättelseinhämtning är verksamhet som ännu inte utgör förberedande av brott eller som inte är straffbar. Den verksamhet som är föremål för militär underrättelseinhämtning kan således vara fullt laglig. En verksamhet kan dock i vissa fall utvecklas till en olaglig verksamhet som avser utredning av brott i takt med att den verksamhet som är föremål för underrättelseinhämtning framskrider. De ovan avsedda situationer som avser utredning av brott ska inte längre höra till den militära underrättelseinhämtningens ansvarsområde utan det är i detta fall fråga om på misstanke om brott grundat militärt kontraspionage eller bekämpning eller utredning av brott.

Föremålen för inhämtande av information inom den militära underrättelseinhämtningen räknas uttömmande upp i paragrafen. Punkterna utesluter inte nödvändigtvis varandra. De kan också vara överlappande och vara aktuella samtidigt.

Ett underrättelseuppdrag som avses i 9 § ska alltid basera sig på de punkter som räknas upp i paragrafen. Ett underrättelseuppdrag kan basera sig på en eller flera punkter som nämns i paragrafen. Det är upp till beslutsfattaren att bedöma om det i en viss situation är motiverat att använda en specifik metod för underrättelseinhämtning och i vilken utsträckning det är motiverat att använda denna metod.

Bestämmelserna i paragrafen styr utarbetandet av underrättelseuppdrag för den militära underrättelseinhämtningen samt användningen av metoder för underrättelseinhämtning. I de bestämmelser om beslutsfattande som det redogörs för nedan förutsätts det att den verksamhet som underrättelseinhämtningen gäller kan preciseras och motiveras. Vid beslutsfattande om metoder för underrättelseinhämtning och genomförande av underrättelseinhämtning ska man dessutom alltid beakta de allmänna principerna, såsom proportionalitetsprincipen och principen om minsta olägenhet samt förbudet mot diskriminering.

Alla föremål för underrättelseinhämtning kan inte klart och tydligt delas in i verksamhet som till sin art är militär och verksamhet som till sin art är civil. Av denna orsak är det ändamålsenligt att den militära och den civila underrättelseinhämtningen kan inhämta information om delvis samma mål. Inhämtandet av information inom den militära och den civila underrättelseinhämtningen kan gälla samma större hotbilder eller helheter, men båda aktörerna ska inhämta information om sitt eget delområde. Om underrättelsemyndigheterna samarbetar kan den högsta statsledningen ges en mer övergripande bild av den helhet som är föremål för observation. Bakgrunden till i synnerhet verksamhet som är föremål för militär underrättelseinhämtning kan vara en främmande stats avsikt att för att nå sina mål påverka en annan stat så att eventuella militära metoder som anses vara traditionella inte behöver användas. En främmande stats påverkan kan också genomföras på så sätt att åtgärderna läggs ut på en aktör utanför den egentliga statliga aktören eller på så sätt att verksamheten som en del av en större krigslist kamoufleras så att den verkar vara brottslig eller terroristisk verksamhet. I synnerhet i dessa situationer kan föremålen för militär och civil underrättelseinhämtning överlappa, och dessutom kan inom samma verksamhetsfält delta också brottsbekämpande myndigheter till följd av sådant inhämtande av information som avser utredning av brott. Detta förutsätter att inhämtandet av information samordnas mellan olika underrättelsemyndigheter. Bestämmelser om militärunderrättelsemyndigheternas samarbete med skyddspolisen och andra myndigheter finns i 16–18 §.

Enligt Europadomstolens etablerade avgörandepraxis ska en lag som begränsar de rättigheter som tryggas i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) ha bl.a. effekter som kan förutses. Förutsebarhet innebär framför allt att lagen är tillräckligt exakt så att det tydligt framgår i vilka förhållanden och under vilka förutsättningar medborgarna kan bli föremål för hemliga myndighetsåtgärder (Weber och Saravia mot Tyskland, punkt 96 och 97).

Europadomstolen har dock ofta påpekat att det redan av ett ärendes karaktär följer att hot mot den nationella säkerheten till sin natur är annorlunda och ibland också oförutsebara, och därför kan det vara svårt att på förhand definiera dessa hot (Kennedy mot Förenade kungariket, punkt 159). Europadomstolens avgörandepraxis behandlas närmare i allmänna motiveringen. Ärendet behandlas närmare i allmänna motiveringen (Europakonventionen).

Strävan med förteckningen över föremål för militär underrättelseinhämtning är att samordna kravet på att lagen ska vara förutsebar och exakt samt behovet av att kunna inhämta information också om nya hot. Europadomstolens ställningstaganden har beaktats när förteckningen utarbetades och det föreslås att bestämmelserna om föremålen för den militära underrättelseinhämtningen ska vara så detaljerade och omfattande som möjligt.

Vilka metoder som kan användas vid inhämtandet av information förutsätter alltid prövning från fall till fall och att den aktör som är föremål för informationsinhämtning identifieras antingen som en statlig aktör eller en annan aktör.

En förutsättning för att en metod för underrättelseinhämtning ska kunna användas är inte att den aktör som ligger bakom verksamheten har identifierats då metoden för underrättelseinhämtning börjar användas. Metoder för underrättelseinhämtning kan användas för att upptäcka hot och identifiera de aktörer som ligger bakom dem. Föremål för en metod för underrättelseinhämtning kan också vara en person eller grupp av personer som kan antas ha samband med verksamhet som avses i denna paragraf.

Tillämpningsområdet för militär underrättelseinhämtning begränsas i 1 mom. till inhämtande av information om verksamhet som till sin art är militär, vilket innebär att verksamheten till sin art inte behöver vara sådan att den utgör ett konkret hot.

Begreppet ”verksamhet som till sin art är militär” definieras inte i lagstiftningen och inte heller i den rättsvetenskapliga litteraturen. Militär verksamhet har granskats i regeringens proposition (RP 172/1999 rd) om ändring av den nu upphävda lagen om försvarsmakten (402/1974) med avseende på vilka ärenden som är militära kommandomål och vilka administrativa mål.

Typiskt för militär verksamhet är stora truppenheter, förberedelser för och ledning av militära åtgärder, militär organisering, deltagande i militär utbildning och militär upprustning i större utsträckning än med stöd av vanliga maktmedelsredskap. Militär verksamhet kräver dessutom ofta omfattande ekonomiska resurser. Det är i allmänhet en stat som ligger bakom en sådan verksamhet.

Militär verksamhet kan bedrivas också av andra än stater. I detta fall ska uppmärksamhet fästas vid verksamhetens planmässighet, ekonomiska resurser och organisering samt vilken form av maktmedel aktören i fråga eventuellt kan tillgripa. En militär icke-statlig aktör kan t.ex. vara en aktör som definierar sig själv som en stat, som andra stater inte har erkänt, eller en separatistgrupp vars verksamhet i betydande grad har samband med en väpnad konflikt. Till exempel en militär styrka utan beteckningar som avses i 2 § i territorialövervakningslagen

(755/2000) anses också vara en icke-statlig aktör, och enligt den paragrafen avses med en sådan styrka en grupp som är jämförbar med militära avdelningar och agerar för en främmande stats räkning eller med en främmande stats samtycke, som är militärt organiserad, utrustad eller beväpnad, och vars statliga ursprung inte kan identifieras. I takt med att tekniken utvecklas kan militära hot riktas mot Finland också från mer avlägsna områden än Finlands närområde.

Enligt 1 mom. 1 punkten i den föreslagna paragrafen får med en metod för underrättelseinhämtning inhämtas information om verksamhet som bedrivs av en främmande stats väpnade styrkor och av med dem jämförbara organiserade trupper samt förberedelse för sådan verksamhet. Verksamheten ska till sin art vara militär i enlighet med det inledande stycket i momentet.

Den verksamhet som avses i punkten är inte begränsad så att den gäller särskilt verksamhet som riktar sig mot Finland. Försvarsmakten ska i stor utsträckning kunna inhämta information om verksamhet som bedrivs av en främmande stats väpnade styrkor och av med dem jämförbara trupper och om utvecklingen av denna verksamhet, trots att verksamheten inte kan anses utgöra ett direkt militärt hot mot Finland. På basis av den information som inhämtats om verksamheten kan det finländska samhället och Försvarsmakten bättre förbereda sig på fientlig verksamhet och denna verksamhets eventuella konsekvenser för Finland.

Verksamhet som bedrivs av en främmande stats väpnade styrkor och av med dem jämförbara trupper inbegriper militära maktmedel och förberedelser för dem, samt militära planer och avsikter. Det som nämns ovan påverkar i väsentlig grad vilken form av reellt hot mot Finland eller andra aktörer som denna verksamhet eventuellt kan utgöra. Ett lyckat inhämtande av information ger mer tid för förberedelser för ett hot. En militär förvarning förutsätter att man ingående kan bedöma olika händelseförlopp. Information om dessa kan t.ex. fås från militär verksamhet på andra håll i världen och granskningar av hur den militära aktören agerar eller har agerat i olika konflikter.

Den förberedelse för verksamhet som nämns i punkten omfattar militärpolitisk och militär utveckling samt militärpolitiska och militära planer. Förberedelser för verksamhet inbegriper t.ex. krigsplaner, gruppering av trupper och utveckling och införskaffning av vapensystem. Utifrån den information som inhämtats försöker man strukturera och minska olika osäkerhetsfaktorer i den säkerhetspolitiska omgivningen samt även utnyttja dem vid försvaret och beredskapen för kriser.

Den verksamhet som avses i punkten är också krig mellan främmande stater eller hot om krig, vilket i väsentlig grad kan påverka också Finlands utrikes- och säkerhetspolitiska relationer eller försvåra Finlands möjligheter att delta i internationellt samarbete.

Till Försvarsmaktens uppgifter hör att som en del av det militära försvaret av Finland trygga den territoriella integriteten. Försvarsmakten ska trygga Finlands territorium, befolkningens livsbetingelser och statsledningens handlingsfrihet samt vid behov försvara den lagliga samhällsordningen med militära maktmedel när ett väpnat angrepp eller ett motsvarande yttre hot riktas mot Finland.

Den verksamhet som avses i punkten omfattar situationer där en främmande stat försöker påverka den demokratiska samhällsordningen i Finland. Med denna verksamhet avses sådana försök att upphäva och förändra samhällsordningen som eventuellt inbegriper våldsamma metoder, hot om våldsamma metoder eller andra förfaranden som strider mot grundlagen.

Hotfull verksamhet kan ta sig uttryck t.ex. som en plan på att använda vapenmakt för att genomföra en intern statskupp eller revolution eller en plan på att göra Finland till en del av en främmande stat. Som hotfull verksamhet kan också anses t.ex. försök att med våld hindra riksdagen att utöva sin lagstiftningsbehörighet eller tvinga personer som utövar regeringsmakt att göra eller låta bli att göra något i sina statliga uppgifter. Bakgrunden till hotfull verksamhet kan vara en främmande stats strävanden, och hotfull verksamhet kan inbegripa drag av militär verksamhet, t.ex. metoder för hybridpåverkan. Information kan inhämtas t.ex. om vilka planer en aktör som ligger bakom de strävanden som nämns ovan har eller vilka förberedelser aktören har vidtagit och vilka personer som från Finland eller utlandet deltar i denna verksamhet.

Till Försvarsmaktens uppgifter hör att skydda Finland mot yttre hot. Detta innebär också att Försvarsmakten inte kan ingripa i Finlands interna ärenden, såsom bl.a. konflikter inom staten och medborgarnas på eget initiativ utövade påverkan i ett demokratiskt samhälle, i form av t.ex. en generalstrejk. Det som nämns ovan ska dock skiljas från en situation som ser ut som en intern konflikt, men som organiseras och stöds av en främmande stat.

Den verksamhet som avses i punkten är också en främmande stats militära och utrikes- och säkerhetspolitiska planer eller verksamhet som kan orsaka skada för Finlands internationella relationer eller andra viktiga intressen. Med en främmande stats verksamhet som orsakar skada avses t.ex. verksamhet som syftar till att på ett fientligt sätt påverka beslutsfattandet i Finland. En främmande stats urval av medel för fientlig påverkan kan vara omfattande och variera i enlighet med det världspolitiska läget mellan allt från politiska och ekonomiska metoder och informationspåverkan till taktisk försummelse av myndighetsverksamhet eller exceptionell aktivering som de faktiska förhållandena inte ger anledning till.

Denna verksamhet har samband med 2 § 1 mom. 1 punkten underpunkt b i lagen om försvarsmakten och enligt den punkten hör till försvarsmaktens uppgifter tryggande av befolkningens livsbetingelser, de grundläggande fri- och rättigheterna och statsledningens handlingsfrihet samt försvar av den lagliga samhällsordningen. En främmande stat kan försöka påverka statsledningens beslutsfattande genom politiska och ekonomiska påtryckningar samt desinformationsoperationer som kan leda till att en främmande makt tillgriper militära maktmedel mot Finland. Genom militär underrättelseinhämtning försöker man reda ut de verkliga avsikterna med denna verksamhet och vilka aktörer som ligger bakom den. Utredning av bakgrunden till olika påtryckningsmetoder har ett direkt samband med att det ska kunna ges en förvarning om att ett militärt hot håller på att utvecklas. Betydelsen av rättidig och objektiv information accentueras vid förberedelser för politiska och ekonomiska påtryckningsmetoder och desinformationsoperationer samt vid förberedelser för det militära hot som eventuellt följer på dessa metoder och operationer. Rättidig och objektiv information möjliggör dessutom att statsledningen kan agera obehindrat när dessa påtryckningsmetoder riktas mot Finland samt hjälper till att förutse utvecklingen av hotet.

En främmande stat kan sträva efter att genomföra sina åtgärder så att målstaten inte kan vara säker på om det är fråga om en målinriktad operation som styrs av en främmande stat eller inte. Sådan verksamhet kan t.ex. vara att man försöker påverka den finska och utländska medborgaropinionen genom att systematiskt sprida felaktig information om Finlands politik i offentligheten. I detta fall kan information inhämtas om huruvida bakgrunden till den informationspåverkan som riktar sig mot Finland är militära strävanden samt om målsättningarna med denna verksamhet.

Verksamhet enligt punkten kan också vara t.ex. en statskupp eller revolution som har inletts eller är inom synhåll i en annan stat, och som ger upphov till ett intresse för hur det politiska

läget i den staten utvecklas. Utvecklingen av det politiska läget kan ha betydande konsekvenser för Finlands utrikes-, säkerhets- och försvarspolitiska läge.

Enligt 1 mom. 2 punkten i den föreslagna paragrafen kan inhämtande av information gälla underrättelseverksamhet som riktar sig mot Finlands försvar.

Enligt den allmänna principen i internationell rätt åtnjuter alla suveräna stater territoriell integritet och politiskt oberoende i förhållande till andra stater. Varje stat beslutar själv om den tillåter och på vilka villkor den tillåter utländska tjänstemän att arbeta inom statens territorium. I allmänna motiveringen konstateras det att de flesta stater de facto upp till en viss gräns tolererar eller till och med godkänner att främmande staters underrättelsemyndigheter är verksamma inom deras territorium. Det kan vara fråga om att informationsutbytet gagnar båda parterna eller att den främmande maktens öppna inhämtande av information om de allmänna förhållandena i målstaten inte äventyrar målstatens eller någon annan aktörs intressen. Under andra förhållanden kan målstaten förhålla sig avvisande till den verksamhet som en främmande stats myndigheter utför inom målstatens territorium. Verksamheten kan också i vissa fall uppfylla rekvisitet för en gärning som är straffbar enligt strafflagstiftningen i målstaten. Verksamhetens straffbarhet kan beroende på målstaten påverkas av t.ex. vem som inhämtar information, vilken information som inhämtas och vilken metod som används för att inhämta information.

Om underrättelseverksamheten riktar sig mot försvaret och om den är framgångsrik, kan denna verksamhet äventyra de intressen som hör till det militära försvaret av Finland och som avses i denna proposition.

Med främmande staters underrättelseinhämtning avses en främmande stats verksamhet som syftar till att främja den egna statens intressen eller att till skada för Finland eller en annan främmande stat inhämta information som målstaten har ett särskilt intresse av att hålla hemlig. Föremål för en främmande stats inhämtande av information kan vara t.ex. Finlands utrikes- och säkerhetspolitik, såsom utvecklingen av Finlands försvar, grunderna för beslutsfattandet, beslutsfattandet på strategisk nivå och militär förmåga, Finlands militära beredskap, samhällets krishanteringsförmåga, försörjningsberedskapen samt teknik på hög nivå och forskning och produktutveckling av den. Utöver informationsinhämtning kan syftet med främmande staters underrättelseverksamhet också vara att påverka bl.a. beslutsfattandet om de ärenden som avses ovan för att främja en främmande stats intressen eller för att skada Finland eller en annan främmande stat.

Med underrättelseverksamhet som riktar sig mot Finlands försvar avses utländsk underrättelseverksamhet där föremål för underrättelseinhämtning är bl.a. organiseringen av försvaret, försvarsförmågan eller den militära teknik som används. De föremål för underrättelseinhämtning som avses ovan har i väsentlig grad också samband med ett intresse av sekretess eftersom strävan kan vara att utifrån den inhämtade informationen på förhand försvaga föremålen för en främmande stats underrättelseinhämtning och de vid behov kan elimineras. Hänvisningen till försvaret medför också att det görs en åtskillnad på föremål för militär underrättelseinhämtning och annan underrättelseverksamhet som traditionellt hör till skyddspolisens behörighet.

Med stöd av de metoder för underrättelseinhämtning som anges nedan kan information inhämtas t.ex. om hur en främmande stats underrättelseinhämtning fungerar med tanke på Finlands försvar, vem som arbetar för eller till förmån för en utländsk underrättelsetjänst eller vilka öppna och hemliga metoderna för inhämtande av information dessa aktörer använder och mot vad metoderna riktar sig. Inhämtandet av information kan gälla också t.ex. vilka mål och prio-

riteringar för inhämtande av information om Finland en främmande stats underrättelsetjänst har fastställt. Med metoder för underrättelseinhämtning kan man också upptäcka och identifiera personer som för en främmande stats underrättelsetjänst avslöjar sekretessbelagd information som är viktig med tanke på försvaret, och personer som en främmande stats underrättelsetjänst försöker rekrytera för sin verksamhet eller som i enlighet med de order och anvisningar de fått från en främmande stats underrättelsetjänst försöker påverka beslutsfattandet till skada för Finland.

Främmande makter och utländska aktörer kan för eget bruk och på ett annat sätt än ett normalt sätt försöka inhämta information om industriellt kunnande som har nära samband med Finlands försvar. Inhämtande av information genom militär underrättelseinhämtning kan gälla t.ex. situationer av detta slag samt utredning av vilken aktör som för eget bruk försöker inhämta information om den finländska försvarsindustrins kunnande.

Underrättelseverksamhet omfattar också situationer där underrättelseinhämtning görs via datanät med hjälp av avancerade sabotageprogram. Underrättelseverksamhet ska ses som teknikneutral och den omfattar alla situationer där målet med verksamheten är att inhämta information om t.ex. de föremål för underrättelseinhämtning som beskrivs ovan och som en främmande stat har intresse av.

Olika stater kan ha organiserat sin underrättelseverksamhet på många olika sätt, såsom framgår av den internationella jämförelsen. Av denna orsak kan det inte anses ändamålsenligt att specificera vilken typ av underrättelsetjänst man kan inhämta information om genom militär underrättelseinhämtning.

Med en metod för underrättelseinhämtning får enligt 1 mom. 3 punkten i den föreslagna paragrafen information inhämtas om planering, tillverkning, spridning och användning av massförstörelsevapen, såsom kemiska och biologiska vapen, toxinvapen samt kärnvapen och radiologiska vapen. Verksamheten ska vara militär till sin art.

Kärnvapen och deras roll vid användningen av maktmedel är på nytt aktuella i den säkerhetspolitiska diskussionen. Spridning av andra massförstörelsevapen och farliga material som hör ihop med dem samt kunnande om dessa vapen och material utgör också ett hot.

Kemiska vapen definieras bl.a. i konventionen om förbud mot utveckling, produktion, innehav och användning av kemiska vapen samt om deras förstöring (FördrS 19/1997). Bestämmelser om biologiska vapen och toxinvapen finns i protokollet rörande förbud för användning i krig av kvävande, giftiga eller liknande gaser samt av bakteriologiska krigsmetoder (FördrS 23/1929), som upprättades i Genève 1925. Bestämmelser om kärnvapen finns bl.a. i fördraget om förhindrande av spridning av kärnvapen (FördrS 11/1970), dvs. det så kallade icke-spridningsavtalet. Definitioner av radiologiska vapen finns t.ex. i den internationella konventionen om bekämpande av bombattentat av terrorister (FördrS 59/2002).

Föremål för underrättelseinhämtning som avser massförstörelsevapen kan vara såväl en person eller grupp av personer som en statlig aktör. Det kan t.ex. vara fråga om inhämtande av information om tillverkning, införskaffning, lagring, innehav eller transport av massförstörelsevapen någon annanstans än i Finland.

En typisk risk som är förknippad med massförstörelsevapen är möjligheten att en mycket stor skada sker. En risk kan anses vara allvarlig också på grund av att skadan är långvarig. En så-

dan risk orsakas t.ex. av en explosion som sprider ut radioaktiva ämnen i miljön på ett tätt bebott område.

Massförstörelsevapen utgör inte nödvändigtvis ett direkt hot mot Finland, men man ska kunna förbereda sig för det hot som de orsakar. Den information som fås om massförstörelsevapen kan dock påverka Finlands möjligheter att agera i internationella forum.

Genom inhämtande av information säkerställs att det finns tillräckliga möjligheter att bekämpa de skador som massförstörelsevapen orsakar. Utifrån den information som inhämtats kan man förbereda sig för att agera i internationella forum och för Försvarsmaktens eventuella deltagande i internationell verksamhet eller militär krishantering.

Att den internationella säkerheten rubbas kan indirekt ha betydelse också för säkerhetssituationen i Finland.

Enligt 1 mom. 4 punkten i den föreslagna paragrafen får med en metod för underrättelseinhämtning information inhämtas om en främmande stats utvecklande och spridning av militärmateriel. Information som inhämtats om den verksamhet som avses i punkten har samband med Försvarsmaktens uppgifter som räknas upp i detaljmotiveringen till paragrafen om syftet med den militära underrättelseinhämtningen.

Information kan inhämtas om såväl en statlig som en icke-statlig aktör eller grupp av aktörer. Det har ingen betydelse vem som utvecklar militärmateriel, utan det är fråga om för vilket ändamål militärmateriel utvecklas. Den verksamhet som avses i punkten är tydligast när den produkt som utvecklas inte kan användas för något annat än militär verksamhet, såsom en missil med tillhörande robotsystem. En situation är dock tydlig också när t.ex. en främmande stats väpnade styrkor har gett en privat aktör i uppdrag att utveckla en viss produkt.

Det är svårare att få klarhet om situationen när en främmande stat inte direkt beställer hela vapensystemet, inklusive alla därmed anslutna delar, av en enskild aktör, utan har delat upp vapensystemets olika delar på flera aktörer. I detta fall ska man bedöma situationen som en helhet och på basis av den erhållna informationen försöka bedöma om alla de delprojekt som fördelats på olika aktörer har samband med utvecklande av ett vapensystem.

Med den militärmateriel som avses i punkten avses teknik som inte utvecklas för att köpas av enskilda personer, utan användarna av militärmateriel är i princip statliga eller med dem jämställbara aktörer som har tillräckliga resurser att skaffa den teknik som avses ovan.

Utvecklande av vapensystem utgör inte nödvändigtvis ett direkt hot mot Finland. Den information som fås om utvecklande av vapensystem har dock en stor betydelse med tanke på Försvarsmaktens verksamhet så att man vid behov effektivt kan skydda sig mot vapensystemen och om hotet realiseras minimera de skador som vapensystemen orsakar.

När underrättelseverksamheten baserar sig på det utvecklande av militärmateriel som avses i denna punkt ska uppmärksamhet alltid fästas vid vilken aktör som utvecklar militärmateriel. Utvecklande av den militärmateriel som behövs vid militär verksamhet kan ske på uppdrag av den privata sektorn. I detta fall är förutsättningarna för användning av metoder för underrättelseinhämtning strängare än när det gäller en statlig aktörs arbete med att utveckla militärmateriel. Man ska också beakta huruvida en stat har direkt bestämmanderätt över en privat aktör som utvecklar militärmateriel och i hur stor grad staten kan styra den aktör som utför utvecklingsarbetet. Ett vanligt kommersiellt avtal mellan en statlig aktör och ett privat bolag kan i

princip inte anses vara ett avtal på basis av vilket den privata aktören kan anses vara en statlig aktör.

Spridning av militärmateriel tyder på att vissa aktörer kan sprida militärmateriel vidare också till små grupperingar som inte nödvändigtvis har resurser att skaffa militärmateriel direkt av tillverkarna. Den information som inhämtas om spridning av militärmateriel har betydelse också i samband med internationellt bistånd och deltagande i militära krishanteringsinsatser. Den inhämtade informationen har i dessa situationer betydelse med tanke på den utrustning som de trupper som skickas till området behöver och deras förberedelser för den verksamhet som sker i området.

Den militärmateriel som avses i punkten samt utvecklande och spridning av den har betydelse för skapande av en militärstrategisk lägesbild samt utvecklande av Finlands säkerhetspolitiska miljö och beredskap för de hot som utvecklandet och spridningen av militärmateriel utgör. Spridningen av militärmateriel höjer risken för att det i en viss stat håller på att bildas en militär aktör eller att en militär aktör i en viss stat blir starkare och äventyrar internationell fred. Spridning av militärmateriel inbegriper också transitering.

Försvarsmaktens uppgifter och militära underrättelseinhämtning gäller dock inte förebyggande och bekämpning av internationell brottslighet, såsom olaglig vapenhandel.

Enligt 5 punkten får det vid militär underrättelseinhämtning inhämtas information om en kris som hotar internationell fred och säkerhet.

Underrättelseinhämtning är med stöd av denna punkt tillåten oberoende av om den som orsakar krisen eller en part i krisen är en statlig eller icke-statlig aktör. Vid sidan av de statliga aktörerna har det uppkommit en expanderande grupp icke-statliga aktörer, vars mål och verksamhetssätt kan utgöra ett hot mot den internationella säkerheten eller enskilda länders och deras invånares säkerhet. Inhämtande av information på basis av denna punkt kan på så sätt förutom verksamhet som eskalerat till en väpnad konflikt gälla också sådan verksamhet som bara är ett förebud om ett hot mot internationell fred. En kris som äventyrar internationell fred och säkerhet och därigenom påverkar behovet av information kan också orsakas av sådana aktörer i olika delar av världen som strävar efter att begränsa de demokratiska institutionernas verksamhet samt inskränka de grundläggande fri- och rättigheterna och mänskliga rättigheterna, yttrandefriheten och aktiviteten på sociala medier.

Finland deltar i internationell krishantering bl.a. för att förebygga och begränsa kriser, avhjälpa de skador som kriserna orsakat och återställa samhällen så att de fungerar ostört samt lindra skador som orsakats av storolyckor eller naturkatastrofer. Förebyggande av konflikter och proaktiv verksamhet ges i nuläget större betydelse. I punkten tillåts av denna orsak underrättelseinhämtning om verksamhet som eventuellt äventyrar krishanteringsinsatser eller personer som deltar i dem. Information kan inhämtas t.ex. på förhand om förhållandena i ett område där en krishanteringsinsats planeras och om faktorer som påverkar säkerheten för de sakkunniga som sänds till området. Inhämtande av information om dessa omständigheter får självfallet fortgå också under insatsen i enlighet med 6 punkten.

Enligt 6 punkten kan föremål för militär underrättelseinhämtning vara verksamhet som hotar säkerheten vid internationella krishanteringsinsatser. Det inhämtande av information som avses i punkten baserar sig på 2 § 1 mom. 4 punkten i lagen om försvarsmakten och 1 § i lagen om militär krishantering (211/2006), och enligt dem kan Finland delta i militär krishantering bl.a. för att upprätthålla eller återställa internationell fred och säkerhet eller för att stödja hu-

manitär hjälpverksamhet eller skydda civilbefolkningen. Bestämmelser om civil krishantering finns i lagen om civilpersonals deltagande i krishantering (1287/2004).

Information kan inhämtas i synnerhet om förhållandena i området där en krishanteringsinsats utförs och om faktorer som påverkar säkerheten för finländska krishanteringsstyrkor, såsom om en våldsam attack hotar finländska sakkunnig som deltar i en krishanteringsinsats och om var, när och på vems uppdrag eventuella våldsdåd kommer att utföras. Inhämtande av information i anslutning till en militär krishanteringsinsats ska ske i enlighet med föreskrifter och anvisningar från den organisation som leder krishanteringsinsatsen.

Inhämtande av information om vilka förhållanden som råder under en krishanteringsinsats kan också ske på förhand, vilket innebär att man till stöd för beslutsfattandet om deltagande i en krishanteringsinsats inhämtar information om förhållandena i området.

Momentets 7 punkt har samband med 2 § 1 mom. 3 punkten i lagen om försvarsmakten. Till försvarsmaktens uppgifter hör enligt 2 § 1 mom. 3 punkten i den lagen deltagande i stöd och bistånd som grundar sig på artikel 222 i fördraget om Europeiska unionens funktionssätt eller artikel 42.7 i fördraget om Europeiska unionen samt deltagande i territorialövervakningssamarbete eller i annat internationellt bistånd och annan internationell verksamhet. Enligt 12 § i lagen om försvarsmakten kan statsledningen besluta om lämnande av bistånd till en annan stat i vissa situationer, såsom till följd av en terrorattack, naturkatastrof, storolycka eller någon annan motsvarande händelse.

Trots att information i första hand fås av den aktör som framställer en begäran om hjälp finns det behov av att information kan inhämtas t.ex. för att kartlägga området där en naturkatastrof inträffat och för att det bistånd som lämnas ska nå fram på ett ändamålsenligt sätt och så säkert som möjligt. Dessutom kan det handla om krävande multinationella evakueringsoperationer, i synnerhet när det är fråga om evakuering av EU-medborgare och evakueringen i övrigt inte kan genomföras t.ex. med hjälp av internationell räddningsverksamhet.

Situationerna kan också inbegripa användning av Europeiska unionens stridsgrupper och Natos snabbinsatsstyrkor i samband med annan krishantering än militär krishantering. Användning av dessa grupper och styrkor är möjlig i alla typer av kriser, också naturolyckor eller olyckor som orsakats av människan.

Militär underrättelseinhämtning kan i enlighet med punkten utföras också i internationellt samarbete vid bekämpning av en väpnad attack till stöd för beslutsfattande enligt klausulen om ömsesidigt bistånd i Lissabonfördraget. Försvarsmakten kan på förhand inhämta information om omständigheter som gäller deltagande i en insats innan beslut fattas om deltagande i en insats som utförs utanför Finlands gränser.

Med den information som inhämtas försöker man också stödja andra finländska myndigheter i deras internationella verksamhet.

Som ett exempel på situationer som avses i punkten kan nämnas att sända finländska specialsakkunniga på specialuppdrag utomlands. Finland kan vid behov sända specialsakkunnig på internationella uppdrag för att förstöra massförstörelsevapen samt analysera användningen av dem. Informationen om utvecklande och spridning av vapen ger Finland en möjlighet att också i framtiden ligga i den internationella toppen i fråga om förstöring och analysering av massförstörelsevapen samt att utveckla detta specialkunnande.

I specialinsatser som gäller förstöring av massförstörelsevapen finns det i den fas när insatsen förbereds ett särskilt behov av underrättelseinformation om t.ex. verksamhetsmiljön och säkerhetshot. När en insats inletts kan man genom underrättelseinformation dessutom säkerställa att målen med insatsen uppnås, t.ex. i fråga om utvecklingen av säkerhetshot som riktar sig mot material som ska förstöras.

En begäran om bistånd kan också gälla deltagande i samarbete med myndigheterna i andra stater för att inhämta information. I dessa situationer kan det vara fråga om en attack som riktar sig mot en stor grupp människor, om attacken kan anses vara militär till sin art. Närmare bestämmelser om internationellt samarbete finns nedan. I dessa situationer ska lagen om beslutsfattande om lämnande av och begäran om internationellt bistånd (418/2017) beaktas.

Enligt 2 mom. i den föreslagna paragrafen får det med militär underrättelseinhämtning inhämtas information om verksamhet som allvarligt hotar det finska försvaret eller samhällets vitala funktioner. Den verksamhet som räknas upp i momentet är till sin art verksamhet som allvarligt hotar den nationella säkerheten i Finland och som inte entydigt är militär verksamhet.

Med begreppet ”nationell säkerhet” avses att den hotfulla verksamhet som nämns i bestämmelsen inte i första hand gäller en enskild individ utan mer allmänt samhället och den mänskliga gemenskapen. Också t.ex. våldsdåd som riktar sig till enskilda personer kan emellertid påverka den nationella säkerheten, om dåden till sin omfattning eller betydelse är relevanta med tanke på den nationella säkerheten och således kan utgöra ett hot mot den. Det är uppenbart att t.ex. hot som riktar sig mot statsledningen eller personer som sköter basfunktionerna i samhället eller mot personer som ansvarar för deras säkerhet kan utgöra ett allvarligt hot mot den nationella säkerheten. Definitionen av nationell säkerhet behandlas närmare i regeringens proposition som gäller ändring av 10 § 3 mom. i grundlagen. I den allmänna motiveringen behandlas hur Europadomstolen i sin avgörandepraxis har förhållit sig till nationell säkerhet och hot mot den samt detta begrepps föränderliga och ibland också oförutsebara karaktär.

Med den hänvisning till det finska försvaret som finns i momentet avses försvaret som helhet genom vilket medborgarnas levnadsmöjligheter och säkerhet tryggas mot yttre hot som orsakas av andra stater eller mot andra hot samt i sista hand Finlands statliga självständighet.

Verksamhet som allvarligt hotar försvaret är verksamhet som t.ex. är så omfattande att den äventyrar Finlands möjligheter att fungera effektivt i en krissituation. Sådan verksamhet kan vara t.ex. ett omfattande och långvarigt angrepp mot datanät för att lamslå Finlands energiförsörjningssystem och till följd av vilket samhället inte kan fungera i en krissituation, vilket försvagar försvarsberedskapen.

Som en del av det finska försvaret betraktas också deltagande i internationella krishanteringsinsatser och givande av internationellt bistånd. Ett undantag från verksamhet som avses i 1 mom. 6 och 7 punkten och 2 mom. kan vara verksamhet som en statlig eller därmed jämförbar aktör inte ligger bakom och som inte kan anses vara militär. Internationella krishanteringsinsatser kan utföras i områden där det inte finns några samhällsstrukturer. I dessa situationer kan en krishanteringsinsats bli föremål för hot, såsom terrorism. Denna typ av verksamhet är inte nödvändigtvis militär till sin art, men den kan ha mycket stor betydelse med tanke på en insats säkerhet.

Enligt 2 mom. i den föreslagna paragrafen kan militär underrättelseinhämtning också gälla verksamhet som allvarligt hotar samhällets vitala funktioner. Detta har ett väsentligt samband med 2 § 1 mom. 1 punkten underpunkt b i lagen om försvarsmakten, och enligt den punkten

hör till försvarsmaktens uppgifter tryggande av befolkningens livsbetingelser, de grundläggande fri- och rättigheterna och statsledningens handlingsfrihet samt försvar av den lagliga samhällsordningen. Samhällets vitala funktioner är förvaltningsövergripande, för samhället nödvändiga helheter som ska vara tryggade i alla situationer. Försvarsmakten ska dessutom också enligt 4 § i lagen om försvarsmakten trygga Finlands territorium, befolkningens livsbetingelser och statsledningens handlingsfrihet samt försvara den lagliga samhällsordningen vid behov med militära maktmedel när ett väpnat angrepp eller ett motsvarande yttre hot riktas mot Finland.

Helheten vitala funktioner inbegriper bl.a. ledningen av staten, internationell verksamhet, militärt försvar av riket, upprätthållande av den interna säkerheten och en fungerande ekonomi och infrastruktur. Verksamhet som äventyrar dessa vitala funktioner är t.ex. verksamhet vars syfte är att i betydande grad försvaga eller lamslå dessa funktioner. Information kan således inhämtas om t.ex. verksamhet som försöker avbryta eller förstöra denna typ av för samhället viktiga funktioner, såsom elproduktion, datakommunikation och datasystem, transportlogistik, samhällsteknik, livsmedelsförsörjning eller finansierings- och betalningssystem.

Allvarliga angrepp mot datatekniska system kan påverka de offentliga tjänsterna, affärslivet och förvaltningen och således hela samhället på ett så betydelsefullt och omfattande sätt att deras konsekvenser i vissa fall kan jämföras med ett väpnat angrepp. Information kan inhämtas t.ex. om förändringar i ägarförhållanden som äventyrar Finlands försörjningsberedskap eller om verksamhet där en främmande stat i datanät kartlägger strukturen på och tekniska sårbarheter i det datatekniska styrsystemet för det europeiska nätverket för energidistribution i syfte att eventuellt utnyttja informationen för att lamslå elnätet.

I verksamhet som allvarligt hotar vitala funktioner kan det vara fråga om t.ex. sabotageprogram som sprids av en privat tjänsteleverantör till de datasystem som myndigheterna använder. Inledande av inhämtande av information om detta kan basera sig på en observation av ett sabotageprogram som gjorts i en annan stat och på basis av vilken den militära underrättelseinhämtningen inhämtar information om huruvida sabotageprogrammet också i Finland har spridits till de datasystem som myndigheterna använder. Dessutom kan information inhämtas om vilken aktör som ligger bakom verksamheten och denna aktörs eventuella avsikter att använda sabotageprogrammet så att det lamslår de datasystem som de finska myndigheterna använder.

Största delen av Finlands kritiska telekommunikationsinfrastruktur och dess tjänster ägs och produceras av den privata sektorn, och därför är den privata sektorns betydelse vid tryggandet av samhällets vitala funktioner viktig. Detta accentueras också vid tryggandet av Finlands försvar. Inhämtande av information gör det möjligt att trygga statsledningens handlingsfrihet samt försvara den lagliga samhällsordningen. Försvarsmakten har specialkunnande om undantagsförhållanden och detta kunnande kan för att säkerställa beredskapen under också andra förhållanden än undantagsförhållanden utnyttjas i de situationer som avses i denna punkt.

Verksamhet som hotar samhällets vitala funktioner riktar sig i första hand inte mot en enskild individ, utan mer allmänt mot staten eller samhället. Till exempel våldsdåd som riktar sig mot enskilda personer kan dock utgöra sådan verksamhet som avses i bestämmelsen, om dåden till sin omfattning och betydelse är relevanta med tanke på samhällets kollektiva säkerhetsintressen och således kan utgöra ett hot mot dem. Med uttrycket hot avses situationer där Finlands säkerhet inte omedelbart håller på att äventyras. Militär verksamhet behöver emellertid inte hota Finlands nationella säkerhet för att bli tillämplig enligt denna bestämmelse. Militär verksamhet kan ha samband med flera av punkterna i paragrafen och med militär verksamhet avses

både statlig och icke-statlig verksamhet (justitieministeriets betänkanden och utlåtanden 41/2016 s. 48 och 49). En militär icke-statlig aktör kan vara t.ex. en terroristorganisation vars verksamhet i betydande grad är kopplad till en väpnad konflikt eller ett inbördeskrig.

**5 §.** *Proportionalitetsprincipen.* Enligt paragrafen ska militärunderrättelsemyndighetens åtgärder vara försvarbara i förhållande till hur viktig informationsinhämtningen är. Målet med proportionalitetsprincipen är att med hänsyn till ett ärendes art begränsa ingripandet i de rättigheter som personer som är föremål för informationsinhämtning har, men att samtidigt rikta myndighetsresurserna på ett ändamålsenligt sätt. Proportionalitetsprincipen styr för sin del all underrättelseverksamhet. Proportionalitetsprincipen inbegriper att man vid dimensioneringen av åtgärderna för inhämtande av information och ingripandet i en persons rättigheter ska beakta hotets betydelse för försvaret och den nationella säkerheten samt sannolikheten för att hotet förverkligas. Det är ändamålsenligt att metoder som i större grad och mer kännbart ingriper i rättigheter används för att inhämta information om ett sådant allvarligt hot mot det finska försvaret eller den nationella säkerheten som sannolikt förverkligas.

En åtgärd för inhämtande av information ska bedömas i förhållande till det eftersträvade målet för åtgärden. Dimensioneringen av åtgärder för inhämtande av information påverkas av t.ex. hur stor betydelse en viss åtgärd har med tanke på inhämtandet av information om ett hot.

Proportionalitetsprincipen inbegriper också kravet enligt grundlagen på att de grundläggande fri- och rättigheterna och de mänskliga rättigheterna ska tillgodoses. Målen med inhämtande av information ska respektera de grundläggande fri- och rättigheterna och de mänskliga rättigheterna för personer som har samband med föremålet för informationsinhämtning. Att underrättelseinhämtningen riktas så bra som möjligt realiserar proportionalitetsprincipen. Underrättelseinhämtningen ska alltid vara så riktad som möjligt och respektera de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. Den prövning som görs med stöd av lagstiftningen om militär underrättelseverksamhet ska alltid beakta de grundläggande fri- och rättigheterna och de mänskliga rättigheterna.

I enlighet med proportionalitetsprincipen ska när en helhetsprövning görs uppmärksamhet fästas vid verksamhetens eller hotets allvarlighet och den skada verksamheten eller hotet eventuellt kan orsaka samt den kränkning av privatlivet eller hemligheten i fråga om förtroliga meddelanden som underrättelseverksamheten innebär.

Vid prövningen av användningen av en åtgärd för inhämtande av information kan det också beaktas hur länge ingripandet i de rättigheter som den person som är föremål för åtgärderna har ska pågå. Om en militärunderrättelsemyndighet redan har information om ett specifikt mål, kan det bli aktuellt med en metod som ingriper mer i en persons rättigheter, om användningen av andra metoder i sig ingriper mindre i personens rättigheter, men samtidigt utgör ett långvarigare ingripande i rättigheterna.

I fråga om proportionalitetsprincipen ska det beaktas att den inte har samma betydelse när det gäller statliga aktörer som vid underrättelseinhämtning som riktar sig mot en militär aktör. Kommunikationen i en främmande stats myndighetsorganisation åtnjuter inget skydd för de grundläggande fri- och rättigheterna. Proportionalitetsprincipen kan dock ha betydelse när det görs en helhetsprövning av hur mycket annan kommunikation än myndighetskommunikation som blir föremål för underrättelseinhämtning i respektive fall av inhämtande av information.

Proportionalitetsprincipen har nära samband med principen om minsta olägenhet i och med att båda principerna syftar till ett så litet ingripande i en persons rättigheter som möjligt.

**6 §.** *Principen om minsta olägenhet.* Principen om minsta olägenhet har samma inverkan som proportionalitetsprincipen. Enligt den princip om minsta olägenhet som avses i paragrafen får det genom användning av underrättelseinhämtningens befogenheter inte ingripas i någons rättigheter i större utsträckning än vad som är nödvändigt för utförande av uppdraget. Militär underrättelseinhämtning får inte heller orsaka någon onödig skada eller olägenhet. För att uppnå målet med inhämtandet av information ska myndigheten i första hand utöva den befogenhet som minst ingriper i de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. Det ska alltid från fall till fall bedömas om befogenheten är tillräcklig.

I enlighet med principen om minsta olägenhet ska av informationsinhämtningens befogenheter alltid i första hand väljas den som bäst kan riktas till ett föremål för underrättelseinhämtning, om vilket det kan inhämtas information som är ändamålsenlig med avseende på underrättelseuppdragets syfte. När principen tillämpas ska också inriktningen av utövandet av en befogenhet beaktas. En så riktad informationsinhämtning som möjligt förhindrar dessutom negativa konsekvenser för utomstående, såsom rädsla för att deras privatliv ska kränkas.

Genom principen om minsta olägenhet tillgodoses för sin del de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. Respekten för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna innebär också att myndigheternas prövningsrätt tydligare än tidigare blir en del av en myndighets prövning i en situation där befogenheter utövas. Principen om minsta olägenhet och de andra principerna begränsar militärunderrättelsemyndighetens egenmäktighet.

Också i fråga om minsta olägenhet ska skillnaderna mellan en statlig och en icke-statlig aktör beaktas i skyddet för de grundläggande fri- och rättigheterna. En främmande stats myndighetsorganisation kan inte anses åtnjuta skydd för de grundläggande fri- och rättigheterna. Av denna orsak får en identifierad främmande stats myndighetsorganisation vara föremål för mer omfattande metoder för underrättelseinhämtning än en enskild person. I helhetsprövningen ska det dock beaktas i vilken utsträckning användningen av en metod för underrättelseinhämtning riktar sig till andra aktörer än en främmande stats myndighetsorganisation. Dessutom kan en företrädare för en främmande stats myndighetsorganisation också en del av tiden vara en enskild person, vilket innebär att personens grundläggande fri- och rättigheter ska tryggas.

**7 §.** *Principen om ändamålsbundenhet.* Enligt paragrafen får den militära underrättelseinhämtningens befogenheter endast utövas för de syften som anges i denna lag.

Principen har att göra med att utövandet av den militära underrättelseinhämtningens befogenheter ska basera sig på en uttrycklig bestämmelse. När man ingriper i en individs rättigheter eller skyldigheter ska det finnas en bestämmelse om detta i lag. Principen om ändamålsbundenhet gäller all militär underrättelseverksamhet.

Principen om ändamålsbundenhet inbegriper ett förbud mot att missbruka makt. Myndigheternas befogenheter får utövas endast för de syften som de har utfärdats för. Enligt principen om ändamålsbundenhet får metoder för underrättelseinhämtning användas endast i underrättelsesyfte för att utföra ett underrättelseuppdrag som avser syftet med och föremålen för den militära underrättelseinhämtningen. Vid brottsbekämpning kan den information som fåtts genom att använda en metod för underrättelseinhämtning användas endast i enlighet med vad som föreskrivs särskilt.

Principen om ändamålsbundenhet accentuerar att en myndighets befogenheter alltid ska basera sig på lag. Detta fullgör för sin del kravet på lagenlighet som följer av grundlagen samt det

krav på att begränsningar ska basera sig på lag som är en förutsättning för begränsningar av de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. Dessutom fullgör principen om ändamålsbundenhet kravet på förutsebarhet eftersom den begränsar utövandet av befogenheterna till endast de situationer som utövandet av befogenheterna är avsett för.

Principen om ändamålsbundenhet har betydelse när proportionaliteten i användningen av metoder för underrättelseinhämtning säkerställs. När användningen av metoder för underrättelseinhämtning begränsas till endast det föreskrivna syftet kan användningen av metoderna inte utvidgas så att de föreskrivna gränserna överskrids.

**8 §.** *Förbud mot diskriminering.* I lagen ska det tas in en princip som är ny i förhållande till de gällande bestämmelserna om andra myndigheters befogenheter. I 8 § föreskrivs det om principen om icke-diskriminering. Principen kan anses motiverad inom underrättelseverksamheten på grund av dess karaktär. Principen innebär dessutom att likställighetsprincipen enligt 6 § 2 mom. i grundlagen stärks inom underrättelseverksamheten.

Enligt paragrafen ska inriktningen av åtgärderna inom den militära underrättelseinhämtningen göras på ett så icke-diskriminerande sätt som möjligt så att underrättelseverksamheten inte enbart får grunda sig på uppgifter om en persons ålder, ursprung, nationalitet, språk, religion, övertygelse, åsikt, politiska verksamhet, fackföreningsverksamhet, familjeförhållanden eller sexuella läggning. Vid inriktningen ska alltid andra uppgifter om vissa personer eller grupper av personer användas. Underrättelseverksamheten ska i princip alltid inriktas på en viss person eller grupp av personer, och då kan inriktningen inte göras på grunder som avser en stor grupp människor.

Inriktning med stöd av de uppgifter som avses ovan kan dock i vissa situationer vara nödvändig, såsom inriktning med stöd av uppgifter om medborgarskap. Detta förutsätter dock objektiva och tillräckliga grunder.

Genom förbudet förhindras diskriminering av minoriteter och den förödmjukelse och känsla av stämpling som detta innebär för representanter för minoriteter.

**9 §.** *Definitioner.* I paragrafen definieras de centrala begreppen i lagen. I 1 punkten i paragrafen definieras begreppet den som utför en koppling. Med den som utför en koppling avses en sådan tillhandahållare av nät- och infrastrukturtjänster som avses i 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015), dvs. aktiebolaget Suomen Erillisverkot Oy, eller ett dotterbolag som helt ägs av tillhandahållaren, dvs. Suomen Turvallisuusverkko Oy. Aktiebolaget ägs helt och hållet av staten med stöd av den paragraf som nämns ovan.

Den som utför en koppling har uppgifter som gäller verkställande av tillstånd för underrättelseinhämtning som avser datatrafik enligt vad som anges nedan, dvs. den som utför en koppling styr datatrafiken från en sådan del av ett kommunikationsnät som avses i ett tillstånd som avses i detta kapitel till Försvarsmaktens underrättelsetjänst, efter vilket Försvarsmaktens underrättelsetjänst i enlighet med tillståndet inhämtar uppgifter om datatrafiken.

Den som utför en koppling kan under verksamhetens gång och utvecklingen av den beräknas få sådan heltäckande information om finska kommunikationsnät och verksamheten i dem som andra aktörer inte kan anses ha. Av denna orsak ska det betonas att den som utför en koppling inte får använda denna information i sin andra verksamhet. Enligt annan lagstiftning som gäl-

ler den som utför en koppling är detta inte heller möjligt och enligt den lagstiftningen får den som utför en koppling inte generera företagsekonomisk vinst.

I 2 punkten i paragrafen definieras lokaliseringsuppgift. Definitionen motsvarar 3 § 18 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014). Med lokaliseringsuppgift avses 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. Lokaliseringsuppgifter kan också fås från en terminalutrustning för att det inte ska bli oklart huruvida bestämmelserna som gäller lokaliseringsuppgifter tillämpas också på t.ex. satellitbaserad lokalisering. Med lokaliseringsuppgifter kan man ange bl.a. en anslutnings eller terminalutrustnings latitud, longitud och höjd, färdriktning, lokaliseringens noggrannhet, den del av nätet där anslutningen eller terminalutrustningen lokaliseras vid en viss tidpunkt samt tidpunkten då lokaliseringsuppgiften sparas. Förmedlingsuppgifter inbegriper också t.ex. lokaliseringsuppgifter enligt basstation. Huruvida en uppgift som anger läge anses vara en förmedlingsuppgift eller en lokaliseringsuppgift avgörs på basis av ändamålet med uppgifterna. Om en uppgift som anger läge används för kommunikation är det fråga om en förmedlingsuppgift. I detta fall är uppgiften som anger en anslutnings eller terminalutrustnings läge nödvändig för att genomföra kommunikationen.

I 3 punkten i paragrafen definieras teleföretag. Definitionen är fristående och motsvarar 3 § 27 punkten i den gällande lagen om tjänster inom elektronisk kommunikation. Med teleföretag avses en aktör som tillhandahåller nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand, dvs. som bedriver allmän televerksamhet. I den föreslagna definitionen av teleföretag fastställs ett teleföretags ställning utifrån verksamhetens art. Med tanke på ett teleföretags ställning har det ingen betydelse om det är fråga om ett företag eller t.ex. en stad. Att verksamheten utförs mot vederlag har inte heller någon betydelse.

Med allmän televerksamhet avses också i fortsättningen tillhandahållande av nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand. Vid bedömningen av om en grupp av användare är avgränsad eller inte ska man beakta t.ex. nätets och tjänstens art, omfattningen av nätet och gruppen av användare och hur restriktiva förutsättningarna för att bli en användare är.

En kommunikationstjänst som ett företag eller en annan sammanslutning upprätthåller för sitt eget behov kan anses vara avsedd för en grupp av användare som tydligt har avgränsats på förhand. De tjänster som t.ex. ett företag erbjuder sina arbetstagare och en skola erbjuder sina elever kan oberoende av hur stor gruppen av användare är eller hur omfattande nätet är inte anses som allmän televerksamhet.

Andra exempel på en avgränsad grupp av användare är en taxicentrals och taxibilars interna kommunikationstjänst för att förmedla taxibilar eller busstrafikens motsvarande interna kommunikationstjänst. I de exempel som beskrivs ovan har tillhörighet till en grupp av användare ett tydligt samband med medlemskap i en sammanslutning som är strängt avgränsad. Av exemplen framgår det också tydligt att orsaken till att man tillhör sammanslutningen inte är kommunikationstjänsten.

De exempel som avses ovan är alltså inte sådana teleföretag som avses i denna lag och de skyldigheter som anges i denna lag gäller således inte dessa aktörer.

Om en grupp av användare av en tjänst däremot utgörs av en sammanslutning som är mycket omfattande eller som man relativt fritt kan gå med i, kan gruppen av användare inte anses ha

avgränsats på förhand. En kommunikationstjänst som t.ex. ett café eller hotell erbjuder sina kunder gäller en grupp kunder som i sig väljs ut mycket fritt, men gruppen av användare är i dessa fall så liten att som helhet kan tillhandahållandet av tjänsten vanligen inte anses vara allmän televerksamhet. Till exempel det faktum att en kommunikationstjänst endast fungerar med en viss applikation eller en viss terminalutrustning innebär däremot i princip inte att gruppen av användare är avgränsad på förhand. Det faktum att ett nät eller en tjänst är tillgänglig endast inom ett visst geografiskt område kan likaså inte i sig anses vara kännetecknande för en grupp av användare som har avgränsats på förhand på det sätt som avses i lagen. Kommunikationstjänster som är bundna till en viss applikation är typiska för t.ex. internetbaserade samtals- och snabbmeddelandetjänster och användarna kan på samma sätt som i fråga om andra produkter fritt skaffa produkterna. Till exempel kommunikationstjänster som hör till en terminalutrustning och är oberoende av mobilföretag ska bedömas på samma sätt, och dessa kan vara t.ex. snabbmeddelanden, e-post och text- och multimediameddelanden.

Nära samband med kommunikationstjänster som är bundna till applikationer har webbforums och sociala mediers olika kommunikationstjänster till vilka man i den grad fritt kan ansluta sig som användare att enbart medlemskap i gemenskapen inte kan anses som att gruppen av användare har avgränsats på förhand.

Man kan med tanke på näten bli tvungen att i fråga om en grupp av användare som inte har avgränsats på förhand bedöma gruppens geografiska täckning i små nät eller förvaltningen av den i nya nät. Till exempel lokalnät, såsom WLAN-nät, som erbjuder internetaccesstjänster kan regionalt erbjuda tjänster inom ett mycket begränsat område, men om lokalnätens användare väljs ut fritt medför en begränsad geografisk täckning inte i sig att gruppen av användare har avgränsats på förhand.

När teleföretag i masskommunikationsnät definieras är bedömningen av en på förhand avgränsad grupp av användare inte på samma sätt en tolkningsfråga som vid målkommunikation eftersom en kommunikationstjänst för masskommunikation, dvs. överföring eller sändning av program, redan till sin art i princip är icke avgränsad. I masskommunikationsnät blir man däremot tvungen att bedöma televerksamheten och innehållet i programverksamheten, dvs. gränsdragningen mellan televisions- eller radioverksamhet och en beställningsprogramtjänst.

I 4 punkten i paragrafen definieras dataöverförare. Med dataöverförare avses den som äger eller innehar en del av ett kommunikationsnät som överskrider Finlands gräns. Definitionen har betydelse för att säkerställa att de i denna lag föreslagna skyldigheterna att bistå myndigheterna vid underrättelseinhämtning som avser datatrafik riktas till rätt aktör. Skyldigheterna att bistå vid underrättelseinhämtning som avser datatrafik gäller å ena sidan den i 95 § i denna lag föreslagna skyldigheten att utan ogrundat dröjsmål lämna Försvarsmaktens underrättelsetjänst de uppgifter som man innehar och som behövs för inriktningen av underrättelseinhämtningen som avser datatrafik. Å andra sidan är det fråga om den i 94 § angivna samarbetsskyldighet som säkerställer att det i en del av ett kommunikationsnät som överskrider Finlands gräns, i praktiken en datakommunikationsförbindelse, kan byggas en så kallad accesspunkt, dvs. en punkt för att genomföra underrättelseinhämtning som avser datatrafik. Via accesspunkter kan det från den del av kommunikationsnätet som avses i domstolens tillstånd överföras datatrafik till Försvarsmaktens underrättelsetjänst för fortsatt behandling. Att göra en koppling och den därpå följande överföringen av datatrafik utgör en del av det tekniska genomförandet av underrättelseinhämtning som avser datatrafik. Vid underrättelseinhämtning som avser datatrafik ska man i det yrkande på tillstånd som framförs till domstolen nämna den dataöverförare som äger eller innehar den del av ett kommunikationsnät från vilken datatrafiken styrs till Försvarsmaktens underrättelsetjänst.

I definitionen används definitionen av kommunikationsnät och därför är definitionen av dataöverförare teknikneutral. Begreppet kommunikationsnät definieras i 11 punkten.

Begreppet dataöverförare omfattar både den som äger en del av ett kommunikationsnät som överskrider Finlands gräns och den som innehar en del av ett kommunikationsnät som överskrider Finlands gräns. Med innehavare avses ett sådant inhemskt eller utländskt företag eller en sådan inhemsk eller utländsk sammanslutning som de facto innehar ett kommunikationsnät som överskrider Finlands gräns eller en del av ett sådant nät, t.ex. genom att hyra det av det företag eller den sammanslutning som äger nätet. En dataöverförare anses således vara en aktör som har tekniska förutsättningar att besluta om i vilken del av ett kommunikationsnät en viss datatrafik sker. Datatekniskt sett är dataöverföraren den part som styr nättrafiken på den nivå som beskrivs av de två lägsta skikten, dvs. det fysiska skiktet och datalänkskiktet, i den så kallade OSI-modellen (Open Systems Interconnection Reference Model). Begreppet dataöverförare omfattar sålunda inte ett företag eller en sammanslutning som av en dataöverförare har hyrt dataöverföringskapacitet utan datateknisk möjlighet att självständigt påverka i vilken del av nätet respektive del av datatrafiken transporteras.

Definitionen är mer detaljerad än t.ex. definitionen av kommunikationsförmedlare i 3 § 36 punkten i lagen om tjänster inom elektronisk kommunikation. Dataöverförare omfattar inte t.ex. företag som erbjuder olika elektroniska tjänster och definitionen omfattar kvantitativt sett färre olika aktörer, vilka när denna proposition överlämnades uppgick till cirka ett tiotal.

Enligt 5 punkten i den föreslagna paragrafen avses med metod för underrättelseinhämtning de befogenheter som militärunderrättelsemyndigheterna har enligt 4 kap. Vid militär underrättelseinhämtning används också andra sådana metoder för inhämtande av information som klassificeras som metoder för underrättelseinhämtning, såsom underrättelseinhämtning ur öppna källor, bildunderrättelser och geografisk underrättelseinhämtning, och som det inte behöver föreskrivas om särskilt.

I 6 punkten i paragrafen definieras underrättelseuppdrag. Utövandet av de befogenheter som anges i lagen baserar sig på utförande av ett visst underrättelseuppdrag och inhämtande av information om det. Med underrättelseuppdrag avses ett uppdrag som Huvudstabens underrättelsechef ger en militärunderrättelsemyndighet för att inhämta underrättelseinformation. Genom underrättelseuppdraget inriktas och avgränsas utövandet av den militära underrättelseinhämtningens befogenheter. Dessutom accentueras underrättelseuppdragets betydelse när det konkretiseras.

Inom militär underrättelseverksamhet syftar underrättelseinhämtningen alltid till ett visst slutresultat, i sista hand till att syftet med den militära underrättelseinhämtningen enligt 3 § förverkligas. Underrättelseuppdraget återspeglar också att verksamheten inte enbart syftar till att inhämta information för informationsinhämtningens skull, utan att underrättelseprocessen alltid ska bidra till ett visst slutresultat, såsom en lägesbild.

Syftet med ett underrättelseuppdrag är alltid att inhämta information om ett föremål för militär underrättelseinhämtning som avses i 4 §. Ett underrättelseuppdrag kan grunda sig på ett eller flera av de föremål som avses i 4 §.

I enlighet med syftet med den militära underrättelseinhämtningen ska det vid militär underrättelseinhämtning inhämtas information om yttre hot för att Försvarsmakten ska kunna utföra vissa av sina uppgifter enligt 2 § i lagen om försvarsmakten samt till stöd för den högsta statsledningens beslutsfattande. Underrättelsebehov som grundar sig på syftet med den militära

underrättelseinhämtningen är Försvarsmaktens interna behov och de baserar sig på Försvarsmaktens uppgifter.

Ett underrättelseuppdrag kan också grunda sig på en annan myndighets begäran om information som det föreskrivs om nedan.

Genom underrättelseuppdraget definieras i mer detalj de konkreta objekt som det ska inhämtas information om så att man kan svara på t.ex. en begäran om information. Genom underrättelseuppdraget definieras med tanke på fullgörandet av ett underrättelseuppdrag mer konkret de ärenden som det ska inhämtas information om samt behoven av information och inriktningen av underrättelseinhämtningen Syftet med ett underrättelseuppdrag kan t.ex. vara utredning av en viss verksamhet som sker inom ett omfattande geografiskt område eller någon annan motsvarande verksamhet som man kan antas behöva information om t.ex. för att svara på en begäran om information.

Ett underrättelseuppdrag ska planeras av Huvudstaben. Den militärunderrättelsemyndighet som utför underrättelseinhämtningen ska inhämta informationen, behandla den inhämtade informationen och analysera den. Huvudstaben deltar med stöd av den inhämtade informationen också i analyseringen av den inhämtade informationen samt svaret på begäran om information.

I underrättelseuppdraget definieras föremålen för användningen av en metod för underrättelseinhämtning inte i detalj på t.ex. personnivå eller i fråga om ett visst utrymme eller område, utan den militärmyndighet som utför inhämtandet av information fastställer dem utifrån underrättelseuppdraget när den verksamhet som inleds på basis av underrättelseuppdraget börjar. Med stöd av underrättelseuppdraget och de mer konkreta föremålen för underrättelseinhämtning fastställer militärunderrättelsemyndigheten från fall till fall de befogenheter som ska utövas för att inhämta den information som behövs.

Militär underrättelseinhämtning tar längre tid än sådant inhämtande av information som avser utredning av brott och t.ex. brottsbekämpning, och underrättelseuppdragen är i princip noga planerade på förhand. Syftet med ett underrättelseuppdrag kan t.ex. vara att samla in information om den verksamhet som utförs av målstatens väpnade styrkor och därmed anslutna omständigheter. Om ett i 4 § avsett föremål för ett underrättelseuppdrag är betydande kan underrättelseuppdraget ta också mycket lång tid.

Trots att själva underrättelseuppdraget kan ta lång tid påverkar detta inte hur länge metoderna för underrättelseinhämtning får användas. Det ska alltid föreskrivas särskilt om användningen av olika metoder för underrättelseinhämtning och deras giltighetstid.

Avsikten med underrättelseinhämtning är inte att förhindra eller reda ut ett enskilt brott utan att samla in information i ett tidigt skede för att få en helhetsbild och säkerställa att en förvarning kan ges.

Enligt definitionen i 7 punkten i den föreslagna paragrafen avses med underrättelseinhämtning som avser datatrafik teknisk informationsinhämtning riktad mot datatrafik i kommunikationsnät som överskrider Finlands gräns. Väsentliga element i definitionen är för det första att underrättelseinhämtningen som avser datatrafik är riktad mot datatrafik som överskrider Finlands gräns och för det andra att gränsen överskrids i ett kommunikationsnät.

Med datatrafik som överskrider Finlands gräns avses att datatrafiken de facto överskrider riksgränsen på så sätt att den överförs från ett finskt kommunikationsnät till ett utländskt kommunikationsnät eller vice versa. Underrättelseinhämtning som avser datatrafik ska tekniskt utföras nära de punkter där Finlands kommunikationsnät och ett utländskt fast nät eller satellitnät är kopplade till varandra och datatrafiken överskrider riksgränsen.

Datatrafik som är avsedd att stanna inom Finlands gränser kan på grund av internets natur slumpmässigt dirigeras via ett utländskt kommunikationsnät. I enlighet med definitionen omfattar denna typ av datatrafik underrättelseinhämtning som avser datatrafik. För att säkerställa att man med underrättelseinhämtning som avser datatrafik trots detta inte inhämtar information om kommunikation som till sitt sakinnehåll är inhemsk ska det nedan föreskrivas om ett förbud mot underrättelseinhämtning som gäller inhemsk kommunikation och enligt vilket underrättelseinhämtning som avser datatrafik bl.a. inte får riktas mot meddelanden vars sändare och mottagare finns i Finland.

I 8 punkten i den föreslagna paragrafen definieras datatrafikens tekniska data. Med datatrafikens tekniska data avses andra uppgifter om datatrafiken än de som hör till innehållet i ett meddelande.

Datatrafikens tekniska data är bl.a. förmedlingsuppgifter om ett meddelande. Begreppet datatrafikens tekniska data är således mer omfattande än begreppet identifieringsuppgifter som definieras nedan. Med förmedlingsuppgifter avses information som kan kopplas till en juridisk eller fysisk person och som den som förmedlar kommunikationen behandlar för att förmedla meddelanden. Vid underrättelseinhämtning som avser datatrafik tolkas som innehåll det semantiska innehåll som avsändaren skickar till mottagaren, medan teknisk data avser t.ex. ett meddelandes styrinformation som inbegriper anvisningar, kommandon eller annan metadata som är avsedda för datanätet samt det avsändande och mottagande datasystemet och som påverkar transporten och styrningen av meddelandet i nätet och datasystemet. Datatrafikens andra tekniska data är uppgifter om den kommunikation som kan kopplas ihop med en abonnent eller användare och vilka behandlas i kommunikationsnätet för att överföra, distribuera eller tillhandahålla meddelanden samt lokaliseringsuppgifter som fås från ett kommunikationsnät eller en terminalutrustning och som anger ett abonnemangs eller en terminalutrustnings geografiska position och används för annat än för att förmedla meddelanden.

En specialfråga när det gäller datatrafik utgör signaleringstrafik inom ett nät, direkt angreppstrafik samt styrningstrafik som gäller det så kallade sakernas internet. I ett datakommunikationsnät är det alltså de facto inte fråga om enbart ett kommunikationsnät där endast meddelandeinnehåll transporteras, utan i nätet transporteras också signalbudskap som påverkar nätverksdriften, styrtrafik för andra digitala system samt direkt angreppstrafik vars syfte är att lamslå nätverksdriften. De viktigaste principerna för utvecklande av internetnät är effektivitet och feltolerans. All trafik, både kommunikation och signalering inom ett nät, transporteras med trafikprotokoll som fastställts i enlighet med samma referensram. Signalbudskap är t.ex. protokoll som används över internet för att signalera olika kontrollfunktioner (ICMP) och genom vilka nätutrustning kan ge varandra lägesrapporter om att en viss länk för datatrafik är överbelastad och om förfrågningar om domännamn genom vilka en meddelandeapplikation reder ut till vilken webbadress ett meddelande som är avsett för ett visst domännamn ska skickas. Det är uppenbart att signaleringstrafik inte kan anses vara kommunikation som åtnjuter skydd för hemligheten i fråga om förtroliga meddelanden. Det är kännetecknande för signaleringstrafik att den kan kännas igen på basis av rubrikuppgifterna.

Sakernas internet medför att ett nät inbegriper styrtrafik som inte heller den i sig kan anses vara kommunikation. Man kan dock inte dra den slutsatsen att den datatrafik som sker mellan utrustning och program utan mänsklig medverkan aldrig utgör kommunikation. Ett typiskt exempel på kommunikation mellan program är ett robotprogram som bedriver börshandel och vars transaktioner har samband med en persons intention att hålla kommunikationen hemlig. Därför har man för styrtrafik som gäller saker i denna lag inte velat ta in en undantagsbestämmelse som möjliggör innehållssökning.

Datatrafikens tekniska data omfattar också i vissa situationer andra tekniska uppgifter, såsom olika krypteringstekniker. I synnerhet stora organisationer som kan vara viktiga med tanke på underrättelseinhämtning kan ha utvecklat sådana egna tekniker för att kryptera datatrafik som används av endast den organisation som har utvecklat tekniken. Uppgifter om krypteringsteknik ger i sig inte information om ett meddelandes betydelsebärande innehåll, utan inbegriper tekniska uppgifter om meddelandet.

Med ett meddelandes betydelsebärande innehåll avses i detta sammanhang den förståeliga texten i meddelandet som man får fram t.ex. genom att dekryptera ett meddelande så att det uttrycks i en språkligt förståelig och läsbar form.

I 9 punkten i den föreslagna paragrafen definieras identifieringsuppgifter. Definitionen av identifieringsuppgifter motsvarar i sak definitionen i den gällande polislagen. Identifieringsuppgifter definieras som 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. Begreppet identifieringsuppgifter avviker således från de förmedlingsuppgifter som avses i lagen om tjänster inom elektronisk kommunikation.

I 10 punkten i paragrafen definieras statlig aktör. Med statlig aktör avses en identifierad myndighet i en främmande stat eller en med en sådan jämställbar aktör. Dessutom omfattar definitionen den som är i en statlig aktörs eller en med en sådan jämställbar aktörs tjänst eller lyder under och styrs av denne. Såsom det har konstaterats tidigare i denna proposition åtnjuter en främmande stats myndighet inget skydd för de grundläggande fri- och rättigheterna. Det kan uppkomma en sådan situation t.ex. när kommunikation sker med utrustning som är avsedd för skötseln av en myndighets myndighetsuppgifter. Om en tjänsteman använder utrustningen för sin privata kommunikation riskerar han eller hon samtidigt att den andra parten i kommunikationen också blir föremål för användning av en metod för underrättelseinhämtning. Utgångspunkten är att utrustning som är avsedd för myndigheternas användning används endast för kommunikation mellan myndigheter.

En aktör som är jämställbar med en myndighet i en främmande stat är också t.ex. en aktör som inte kan identifieras som en myndighet, men som sköter statens ärenden som en myndighet. En aktör kan bedömas t.ex. i fråga om huruvida Finland eller en finsk myndighet kan ingå ett avtal med aktören eller om aktören kan delta i en internationell organisations verksamhet.

En statlig aktör kan dock också vara en privat aktör, såsom ett företag, en annan sammanslutning eller till och med en enskild person. I dessa fall är det fråga om en aktör som agerar på uppdrag av en myndighet, dvs. en så kallad mellanhand, och arbetar för en statlig aktörs räkning. I detta fall är det viktigt att bedöma t.ex. om denna aktör lyder under och styrs av staten eller om staten själv tar ansvar för denna aktörs verksamhet. Till exempel de skyldigheter som ett företag har gentemot en statlig aktör och som baserar sig på ett kommersiellt privaträttsligt avtal kan inte anses vara sådana att ett företag kan anses vara en statlig aktör. Det bör beaktas

t.ex. vilken form av faktisk bestämmanderätt staten har över företaget och vilken möjlighet staten har att styra företaget och hur konkret staten kan bestämma om företagets verksamhet.

I fråga om andra sammanslutningar ska uppmärksamhet utöver vid det som nämns ovan också fästas vid hur organiserad verksamheten är, och hur betydande resurser sammanslutningen har till sitt förfogande t.ex. för att genomföra ett väpnat angrepp, och om konsekvenserna av ett sådant angrepp kan jämställas med ett angrepp av en främmande stat samt om sammanslutningen strävar efter att agera på samma sätt som en stat.

Det är en självklarhet att en statlig aktör på förhand ska ha identifierats som en statlig aktör. Detta innebär t.ex. att militärunderrättelsemyndigheten när den fattar beslut om användning av en metod för underrättelseinhämtning eller utarbetar ett tillståndskrav har förhandsuppgifter om att föremålet för underrättelseinhämtning är en statlig aktör som under den tid metoden för underrättelseinhämtning används agerar i denna roll. Under den tid ett underrättelseuppdrag pågår kan användningen av en metod för underrättelseinhämtning till en början vara något annat än informationsinhämtning som riktar sig mot en statlig aktör, men kan i en senare fas med stöd av den information som fåtts genom metoden för underrättelseinhämtning fortsätta som användning av en metod för underrättelseinhämtning som riktar sig mot en statlig aktör, om det framgår att aktören har samma status som en statlig aktör. I sista hand är det den som fattar beslut som ska avgöra om det som stöd för ett yrkande har lagts fram tillräckliga bevis för att den aktör som är föremål för underrättelseinhämtningen kan anses vara en statlig aktör.

Enligt 11 punkten i den föreslagna paragrafen avses med 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.

Väsentligt med tanke på definitionen är att systemet är avsett för överföring eller distribution av meddelanden och att det verkställs tekniskt på ett elektromagnetiskt sätt och att det är teknikneutralt. Till ett kommunikationsnät hör t.ex. överföringssystem samt utrustning för koppling och dirigering och andra verktyg – också nätdelar som inte är aktiva. Definitionen är ett överordnat begrepp för de andra kommunikationsnät som används i lagen och som enligt förslaget är masskommunikationsnät, markbundna masskommunikationsnät, kabeltelevisionsnät och mobilnät.

Enligt 12 punkten i den föreslagna paragrafen avses med sammanslutningsabonnent en i 3 § 41 punkten i lagen om tjänster inom elektronisk kommunikation avsedd sammanslutningsabonnent. Med sammanslutningsabonnent avses enligt 3 § 41 punkten i den lagen ett företag eller en organisation som abonnerar på kommunikationstjänster eller mervärdestjänster och som i sitt kommunikationsnät behandlar meddelanden från användare samt förmedlingsuppgifter och lokaliseringsuppgifter.

**10 §.** *Militärunderrättelsemyndigheter.* I 1 mom. definieras militärunderrättelsemyndigheter. Huvudstaben svarar för den militära underrättelseinhämtningen i sin helhet och ledningen av den samt styrningen av den inom Försvarsmakten. Försvarsmaktens organisationsstruktur grundar sig på lagen om försvarsmakten, försvarsministeriets förordning om försvarsministeriets arbetsordning samt andra författningar. Enligt Huvudstabens arbetsordning svarar Huvudstabens underrättelseavdelning för skötseln av uppdragshelheten militär underrättelseinhämtning.

Till ansvarsområdet militär underrättelseinhämtning hör militär underrättelseinhämtning samt militärt kontraspionage som inbegriper inhämtande av information, behandling av information samt rapportering. Huvudstaben leder Försvarsmaktens underrättelsetjänst och försvarsgrenarnas underrättelseinhämtning samt det nationella och internationella samarbetet inom den militära underrättelseverksamheten.

Användningen och inriktningen av den militära underrättelseinhämtningens resurser styrs i första hand av de riktlinjer som dragit upp vid det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president. På basis av prioriteringarna beslutar Huvudstaben om behandlingen av en enskild begäran om information som lämnats av den högsta statsledningen eller den militära ledningen. Huvudstaben deltar i analyseringen av och rapporteringen om den information som inhämtats med metoder för underrättelseinhämtning.

Den myndighet som utövar den militära underrättelseinhämtningens befogenheter är Huvudstaben, dvs. Huvudstabens underrättelseavdelning, och Försvarsmaktens underrättelsetjänst som med olika metoder för underrättelseinhämtning inhämtar behövlig information, analyserar den samt rapporterar den vidare. Försvarsmaktens underrättelsetjänst är en militär inrättning som är direkt underställd Huvudstaben och som styrs av Huvudstaben.

Huvudstabens underrättelseavdelning utövar redan i nuläget befogenheter i anslutning till brottsbekämpning med stöd av lagen om militär disciplin och brottsbekämpning inom försvarsmakten. De metoder för inhämtande av information som används vid brottsbekämpning är delvis jämförbara med de befogenheter som föreslås i denna lag. Denna erfarenhet kan utnyttjas i den nya militära underrättelseverksamheten, dock så att den militära underrättelseverksamheten differentieras från brottsbekämpning.

Militärunderrättelsemyndigheten utför informationsinhämtning som baserar sig på ett underrättelseuppdrag som grundar sig på en begäran om information samt utreder och analyserar den information som inhämtats. Militärunderrättelsemyndigheterna lämnar utifrån detta Huvudstaben en slutprodukt som uppfyller kraven i begäran om information och som Huvudstaben efter att ha behandlat lämnar vidare till den myndighet som begärt information.

Huvudstabens underrättelsechef och i synnerhet för uppdraget förordnade och med användningen av metoder för underrättelseinhämtning förtrogna tjänstemän beslutar i stor utsträckning om utövandet av de befogenheter som föreskrivs i denna lag.

Militärunderrättelsemyndigheterna får annat stöd för underrättelseinhämtning än stöd för användning av metoder för underrättelseinhämtning också av andra enheter inom Försvarsmakten och av gränsbevakningsväsendet. Försvarsgrenarnas och gränsbevakningsväsendets stöd baserar sig på i synnerhet den information som inhämtas för att utföra deras territorialövervakningsuppdrag och den information som behövs för den underrättelseinhämtning som inhämtas inom den egna verksamheten. Inom flygvapnet och marinen stöder territorialövervakningen underrättelseverksamheten och vice versa. Också Försvarshögskolan och Försvarsmaktens forskningsanstalt utför forskning och analyser som är till nytta för militär underrättelseinhämtning. Dessutom kan militärunderrättelsemyndigheten få viktig information av t.ex. Försvarsmaktens logistikverk, vars anställda arbetar aktivt med upphandling av krigsmateriel. Det är inte fråga om egentlig underrättelseinhämtning, utan information som är betydelsefull med tanke på underrättelseinhämtning fås vid sidan av de normala arbetsuppgifterna.

I fråga om gränsbevakningsväsendet bör det dessutom beaktas att om försvarsberedskapen kräver det kan gränsbevakningsväsendets gränstrupper eller delar av dem anslutas till Försvarsmakten genom förordning av republikens president. I dessa situationer utgör gränsbevakningsväsendet en del av Försvarsmaktens organisation och när gränsbevakningsväsendet deltar i militär underrättelseverksamhet blir bestämmelserna i denna lag tillämpliga.

I vissa situationer är det ändamålsenligt att Försvarsmaktens trupper som fått specialutbildning används i underrättelseinhämtningens biträdande uppgifter. Dessa trupper har specialutbildning i användning av metoder för underrättelseinhämtning och trupperna är i dessa uppgifter underordnande militärunderrättelsemyndigheten. En militärunderrättelsemyndighet som använder dessa trupper är ansvarig för en trupps verksamhet.

Också reservister ska kunna användas i vissa fall. Under värnpliktstjänsten utbildas en del av de värnpliktiga i uppgifter inom militär underrättelseinhämtning. Reservister kan i större utsträckning användas främst i situationer där man fått information som stöder en sådan effektivisering eller höjning av beredskapsläget som ännu inte kräver att andra reservister än reservister som är utbildade för underrättelseinhämtning inkallas till en repetitionsövning, men där det behövs tilläggsresurser för militär underrättelseinhämtning för att inhämta information om utvecklingen av en verksamhet som hotar Finland. Det föreskrivs nedan om reservisters deltagande.

I enlighet med 2 mom. i den föreslagna paragrafen kan försvarsgrenarna använda radiosignalspaning i det syfte som avses i denna lag, såsom föreskrivs nedan. På beslutsfattandet tillämpas dock samma bestämmelser som i övrigt gäller för utövandet av befogenheter. I situationer där försvarsgrenarna utför militär underrättelseinhämtning sker verksamheten under ledning och övervakning av militärunderrättelsemyndigheterna. Försvarsgrenarna ska lämna vidare den information de samlat in till Huvudstaben som analyserar den och vidarebefordrar den till den myndighet som begärt information.

**11 §.** *Allmänna förutsättningar för användning av metoder för underrättelseinhämtning.* I 1 mom. föreskrivs det om en för alla metoder för underrättelseinhämtning gemensam förutsättning för användning, dvs. att ”det med fog kan antas att man genom metoden kan få information med avseende på ett underrättelseuppdrag”. Det är fråga om ett krav på resultat som förutsätter en motivering, vilket innebär att väntevärdet för användningen av en metod för underrättelseinhämtning är dess användbarhet för att få information om den verksamhet som är föremål för den militära underrättelseinhämtningens underrättelseuppdrag. Användbarheten i fråga om användningen av en metod för underrättelseinhämtning ska i varje enskilt fall kunna motiveras, vilket uttrycks med begreppet ”med fog”. Motiveringen kan gälla t.ex. varför uttryckligen en viss person eller grupp av personer eller ett visst utrymme eller någon annan plats ska kunna övervakas och varför man på detta sätt kan antas få nyttig information. Med verksamhet som är föremål för den militära underrättelseinhämtningens underrättelseuppdrag avses verksamhet enligt 4 § (föremål för den militära underrättelseinhämtningen).

Inom militär underrättelseinhämtning kan ett underrättelseuppdrag basera sig på verksamhet som till sin art är militär och avses i 4 § 1 mom. Den verksamhet som räknas upp i momentet behöver inte utgöra ett hot mot Finland eller den nationella säkerheten. Som grund för användningen av en metod för underrättelseinhämtning räcker i detta fall att man genom metoden får information om verksamheten.

Till skillnad från det som nämns ovan utgör den verksamhet som avses i det föreslagna 4 § 2 mom. ett allvarligt hot mot Finlands nationella säkerhet. Som grund för användningen av en

metod för underrättelseinhämtning räcker i dessa situationer inte enbart ett abstrakt hot utan det ska i varje enskilt fall kunna visas att den verksamhet som avses i 4 § 2 mom. verkligen hotar eller kan antas hota den nationella säkerheten. I fråga om t.ex. ett sabotageprogram som kan lamslå energiinfrastrukturen och som observerats någon annanstans än i Finland kan det i många fall antas att verksamheten kan utvidgas också till Finlands territorium.

Uttrycket ”det med fog kan antas” motsvarar i fråga om graden av sannolikhet uttrycket ”finns skäl att anta” eller ”finns skäl/anledning att misstänka” som i nuläget används i samband med befogenheter som avser utredning av brott och som anger graden av sannolikhet för att bl.a. hemliga tvångsmedel ska få användas. Den minsta graden av sannolikhet beskrivs i nuläget av uttrycket ”finns skäl att anta” som t.ex. i 7 kap. 1 § i tvångsmedelslagen beskriver förutsättningar för beslag. Ett uttryck som används parallellt med ”finns skäl att anta” är t.ex. uttrycket ”finns anledning att misstänka” som används i tvångsmedelslagens 6 kap. 1 § som gäller förutsättningar för kvarstad. Detta alternativa uttryck används då det är fråga om mänsklig verksamhet som antingen redan har inträffat (t.ex. ett brott) eller som antas kunna inträffa i framtiden (t.ex. undvikande av förundersökning). I förundersökningslagens 3 kap. 3 § 1 mom. som gäller skyldighet att göra förundersökning används uttrycket ”finns skäl att misstänka”. Enligt motiveringen (s. 16) till regeringens proposition (RP 14/1985 rd) som gäller den lagen finns det skäl att misstänka ett brott när en omsorgsfull person på grund av sina iakttagelser kommer till en sådan slutsats.

Användningen av en metod för underrättelseinhämtning ska dessutom kunna riktas så exakt som möjligt. Detta krav beror på de allmänna principerna för militär underrättelseinhämtning, i synnerhet principen om minsta olägenhet. Inriktningen ska dessutom motiveras separat i det beslut eller tillstånd som gäller en metod för underrättelseinhämtning, vilket det föreskrivs om nedan.

Förutsättningarna för användningen av en metod för underrättelseinhämtning är graderade. Särskilda förutsättningar fastställs separat för varje metod för underrättelseinhämtning. Att förutsättningarna för användningen av en metod för underrättelseinhämtning är graderade motsvarar det som i 89 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten och i 5 kap. 2 § i polislagen föreskrivs om hemliga metoder för inhämtande av information.

I fråga om användningen av metoder för underrättelseinhämtning som kraftigt begränsar de grundläggande fri- och rättigheterna för den person som är föremål för underrättelseinhämtning föreskrivs ytterligare förutsättningar separat för varje metod för underrättelseinhämtning. Till skillnad från de gällande bestämmelserna ska det separat för varje metod för underrättelseinhämtning föreskrivas om särskilda förutsättningar för utövandet av befogenheter. Att särskilda förutsättningar anges enligt befogenhet förtydligar systematiken i bestämmelserna och ger lagtillämparen en tydligare bild av förutsättningarna för utövandet av en befogenhet.

Användningen av metoder för underrättelseinhämtning kan inledas med att lindrigare metoder för underrättelseinhämtning används och att metoder som ingriper mer i de grundläggande fri- och rättigheterna börjar användas enligt behov i takt med att inhämtandet av information framskrider.

Om militärunderrättelsemyndigheten däremot har tillgång till tillräckligt exakta uppgifter om föremålet för underrättelseinhämtning när ett underrättelseuppdrag inleds kan det redan i utgångsläget bli aktuellt med utövande av befogenheter som ingriper mer i de grundläggande fri- och rättigheterna.

När användningen av metoder för underrättelseinhämtning övervägs ska också de allmänna principerna samt förbudet mot diskriminering alltid beaktas. Användningen av en metod för underrättelseinhämtning kan redan i utgångsläget i betydande grad ingripa i de grundläggande fri- och rättigheterna för den aktör som är föremål för underrättelseinhämtning, men metoden kan vara acceptabel med tanke på de allmänna principerna, om den i övrigt orsakar föremålet och utomstående mindre skada.

När metoder för underrättelseinhämtning används har principerna för militär underrättelseinhämtning en accentuerad betydelse då föremålet för underrättelseinhämtning är en aktör som åtnjuter skydd för de grundläggande fri- och rättigheterna. Respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna, proportionalitet och strävan efter minsta olägenhet är alla viktiga principer också när metoder för underrättelseinhämtning används. Att dessa principer iakttas säkerställer i sig att tolkningen av förutsättningarna för användningen av metoder för underrättelseinhämtning håller sig inom de tillåtna gränserna och styr militär-underrättelsemyndigheten så att den använder den metod för underrättelseinhämtning som är mest ändamålsenlig.

Grundlagsutskottet har i sina utlåtanden (GrUU 32/2013 rd, s. 4 och GrUU 33/2013 rd, s. 4) ansett att de allmänna principerna i polislagen och tvångsmedelslagen liksom även de allmänna och särskilda förutsättningarna för användning av hemliga metoder för inhämtande av information 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). Till skillnad från i de lagar som avses ovan är det inte möjligt att gradera förutsättningarna för användning av metoder för underrättelseinhämtning på basis av hur allvarliga brotten är eftersom underrättelseverksamheten inte gäller brott. Detta gör att beslutsfattaren i större utsträckning måste bedöma villkoren i ett tillstånd som gäller rätt att inhämta information. För att beslutsfattaren i dessa fall ska ha möjlighet att noggrant överväga behovet av att bevilja tillstånd och tillståndets omfattning ska beslutsfattaren ha tillgång till tillräcklig information. Dessutom betonas vikten av extern övervakning.

När tillstånd beviljas och befogenheter utövas ska i sista hand en helhetsbedömning tillämpas där också proportionalitetsprincipen och principen om minsta olägenhet ska ges betydelse.

Användningen av metoder för underrättelseinhämtning ska alltid basera sig på ett underrättelseuppdrag som beskrivs närmare i detaljmotiveringen till 9 §. Ett underrättelseuppdrag ska alltid ha samband med prioriteringarna i den militära underrättelseinhämtningen och föremålen för militär underrättelseinhämtning. Utöver de förutsättningar som avses ovan ska det särskilt för varje enskild metod för underrättelseinhämtning föreskrivas om hur länge metoden för underrättelseinhämtning får användas samt om de omständigheter som ska anges i en tillståndsansökan eller ett beslut. I t.ex. en tillståndsansökan för teleavlyssning ska för domstolen läggas fram bl.a. de fakta som utgör grund för förutsättningarna för teleavlyssning eller för det inhämtande av information som utförs i stället för teleavlyssning samt inriktningen av teleavlyssning.

Vid användningen av metoder för underrättelseinhämtning accentueras betydelsen av de allmänna principerna enligt lagen om militär underrättelseverksamhet. Utöver den grundlagsenliga respekten för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna är också proportionalitetsprincipen, strävan till minsta olägenhet, principen om ändamålsbundenheten och förbudet mot diskriminering alla viktiga principer när metoder för underrättelseinhämtning används. Att dessa principer iakttas vid militär underrättelseinhämtning säkerstäl-

ler att tolkningen av förutsättningarna för användningen av metoder för underrättelseinhämtning håller sig inom de tillåtna gränserna.

I 2 mom. i den föreslagna paragrafen föreskrivs det om de särskilda förutsättningar för användning av metoder för underrättelseinhämtning som ingriper i skyddet för förtroliga meddelanden när föremålet för underrättelseinhämtning är en verksamhet som avses i 4 § 2 mom. Utöver de särskilda förutsättningar som räknas upp i momentet ska det separat för varje metod för underrättelseinhämtning dessutom föreskrivas om förutsättningarna för användning.

En förutsättning för att de metoder för underrättelseinhämtning som avses i momentet ska kunna användas är att den verksamhet som avses i 4 § 2 mom. utgör ett ”allvarligt hot” mot den nationella säkerheten. Detta krav följer direkt av 10 § 3 mom. i grundlagen. Detta moment i grundlagen innebär att kravet på allvarlighet höjer tröskeln för att tillämpa metoder som ingriper i skyddet för förtroliga meddelanden när arten av ett kvalificerat hot fastställs. Enbart verksamhet som utgör någon form av hot mot den nationella säkerheten uppfyller således inte ännu det krav som ställs i bestämmelsen. Ett hots allvarlighetsgrad är också förenat med de i 4 § 2 mom. behandlade innehållsliga definitioner av hurdan den verksamhet som är föremål för militär underrättelseinhämtning ska vara för att utgöra ett hot mot den nationella säkerheten.

Uttrycket ”nationell säkerhet” innebär att den hotfulla verksamhet som avses i bestämmelsen inte i första hand riktar sig mot en viss individ utan mer allmänt mot samhället och den mänskliga gemenskapen. Också t.ex. våldsdåd som riktar sig mot enskilda personer kan dock utgöra en sådan verksamhet som avses i bestämmelsen, om dåden till sin omfattning eller betydelse är relevanta med tanke på den nationella säkerheten och således kan utgöra ett allvarligt hot mot den. Det är uppenbart att t.ex. hot som riktar sig mot statsledningen eller personer som sköter grundläggande samhällsfunktioner eller mot personer som svarar för deras säkerhet kan utgöra ett allvarligt hot mot den nationella säkerheten. Definitionen av nationell säkerhet behandlas närmare i regeringens proposition som gäller ändring av 10 § i grundlagen. I den allmänna motiveringen behandlas hur Europadomstolen i sin avgörandepraxis har förhållit sig till nationell säkerhet och hot mot den samt detta begrepps föränderliga och ibland också oförutsebara karaktär.

Som grund för användningen av de metoder för underrättelseinhämtning som avses i momentet räcker dock inte enbart ett abstrakt hot utan det ska i varje enskilt fall på reell nivå kunna visas att en verksamhet som är föremål för militär underrättelseinhämtning utgör ett allvarligt hot eller kan antas utgöra ett allvarlig hot mot den nationella säkerheten. Med uttrycket ”hot” avses att det i bestämmelsen inte förutsätts att den nationella säkerheten direkt äventyras. På så sätt kan den användning av metoder för underrättelseinhämtning som avses i bestämmelsen gälla en verksamhet som är föremål för militär underrättelseinhämtning och som om den tillåts fortgå allvarligt hotar den nationella säkerheten. Det förutsätts dock att ett hot är på något sätt nära förestående eller så bör det åtminstone indirekt ha en koppling till Finlands nationella säkerhet.

Utöver i fråga om teknisk avlyssning, teleavlyssning av någon annan än en statlig aktör, inhämtande av information i stället för teleavlyssning, teleövervakning av någon annan än en statlig aktör, kopiering av en försändelse och underrättelseinhämtning som avser någon annan aktörs datatrafik än en statlig aktörs datatrafik är också förutsättningarna för användning av kopiering strängare när kopieringen riktas mot ett meddelande. Med ett meddelande avses de förtroliga meddelanden som skyddas i 10 § i grundlagen. Kopiering riktas mot ett meddelande t.ex. när ett brev som lämnats på ett bord eller ett e-postmeddelande på en datorskärm är före-

mål för kopiering. En förutsättning för att ett foto ska få tas eller någon annan form av kopiering ska få göras är i dessa fall det som föreskrivs i första meningen i momentet.

Liksom det konstateras nedan är tröskeln lägre för användning av sådana metoder för underrättelseinhämtning som riktas mot en statlig aktör. Användningen av metoder för underrättelseinhämtning ska kunna riktas mot kommunikationen mellan två statliga aktörer som inte åtnjuter skydd för förtroliga meddelanden enligt grundlagen. En sådan situation kan uppkomma t.ex. om kommunikationen sker i ett myndighetsnät. Om en tjänsteman använder ett myndighetsnät för att ringa privata samtal så riskerar han eller hon samtidigt att den så kallade B-abonnenten, dvs. en aktör som inte är föremål för användningen av en metod för underrättelseinhämtning, också blir föremål för underrättelseinhämtning. Utgångspunkten är att myndighetsnät används för kommunikation mellan myndigheter.

I 3 mom. i den föreslagna paragrafen fastställs det att metoderna för underrättelseinhämtning enligt denna lag får användas i hemlighet för dem som är föremål för metoderna. Med detta avses att en myndighet som använder en metod för underrättelseinhämtning inte separat behöver meddela föremålet för underrättelseinhämtning eller utomstående om att det t.ex. på ett område eller i ett utrymme utförs militär underrättelseinhämtning. Om en person utan grund eller i övrigt har blivit föremål för användning av metoder för underrättelseinhämtning ska denna underrättas om detta i efterhand på det sätt som föreskrivs i 86 §. En person har dessutom tillgång till de metoder att bevaka sina rättigheter som avses i lagen om övervakning av underrättelseverksamhet.

Enligt 4 mom. i den föreslagna lagen ska användningen av en metod för underrättelseinhämtning avslutas före utgången av den tid som anges i beslutet, eller tillståndet så snart syftet med användningen har nåtts det inte längre finns förutsättningar för användningen av metoden. Metoder för underrättelseinhämtning får under inga omständigheter användas under en längre tid än vad som är nödvändigt trots att tillståndet ännu är i kraft. Det säger sig självt att användningen av en metod för underrättelseinhämtning ska avslutas senast då tillståndets giltighetstid upphör.

## 2 kap. Styrning av och tillsyn över den militära underrättelseinhämtningen

**12 §.** *Styrning och ledning av den militära underrättelseinhämtningen.* I 1 mom. föreskrivs det om styrning av den militära underrättelseinhämtningen med hjälp av de prioriteringar som behandlats förberedelsevis av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president. De årliga prioriteringarna ska behandlas förberedelsevis av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president.

I det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president deltar utöver republikens president också andra aktörer som är viktiga med tanke på utrikes- och säkerhetspolitiken. Ledamöter i utrikes- och säkerhetspolitiska ministerutskottet är enligt 25 § 1 mom. i reglementet för statsrådet statsministern, utrikesministern, försvarsministern samt fyra andra ministrar som statsrådet förordnar. Enligt 2 mom. i den paragraf som avses ovan inbjuds också inrikesministern till mötet om frågor som har samband med ministerns ansvarsområde behandlas.

Med de prioriteringar som behandlas förberedelsevis av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president avses långsiktiga utvecklingslinjer som med tanke på utrikes- och säkerhetspolitiken är viktiga för Finland och

som det behövs närmare information om till stöd för den högsta statsledningens beslutsfattande. Prioriteringarna kan gälla t.ex. ett visst område eller en viss ärendehelhet. Det är inte fråga om enstaka militära hot eller sporadisk militär verksamhet eller enstaka hot som äventyrar Finlands nationella säkerhet.

Prioriteringarna kan också påverkas av kortvariga händelser och utvecklingstrender. Om denna typ av utvecklingstrender har konsekvenser kan prioriteringarna vid behov anpassas genom att de nya prioriteringarna behandlas förberedelsevis av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president.

De prioriteringar som behandlats förberedelsevis av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president ska av försvarsministeriet behandlas på samma sätt som man hittills gjort med de ärenden som behandlats vid dessa möten. Arbetsformerna ändras inte till denna del.

I prioriteringarna tas det inte ställning till hur och med stöd av vilka befogenheter information inhämtas. Till följd av de allmänna principer som styr militärunderrättelsemyndighetens verksamhet och bestämmelserna om inriktning av utövandet av befogenheter är verksamheten inom den militära underrättelseinhämtningen noggrant avgränsad genom lag. Detta betyder också t.ex. att om sammansättningen i det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president ändras på grund av en förändring i det politiska läget i Finland påverkar det inte hur, varifrån och under vilka förutsättningar information kan inhämtas genom militär underrättelseinhämtning. Dessutom ska justitiekanslerns roll i ärenden som gäller tillsynen över statsrådet beaktas när det gäller både principiella och vittomfattande ärenden. I sista hand ansvarar Huvudstabens underrättelsechef och militärunderrättelsemyndigheterna för att man vid den militära underrättelseinhämtningen har agerat lagenligt.

I fråga om styrningen gäller utöver det som nämns ovan också det som i 31 och 32 § i lagen om försvarsmakten föreskrivs om beslutsfattandet i militära kommandomål.

Enligt 2 mom. i den föreslagna paragrafen styr försvarsministeriet den militära underrättelseinhämtningen administrativt. Trots att försvarsministeriets styrande roll baserar sig på lagen om statsrådet och reglementet för statsrådet (262/2003) är det på grund av den militära underrättelseverksamhetens betydelse och omfattning ändamålsenligt att det uttryckligen föreskrivs om detta. Avsikten med bestämmelsen är inte att påverka försvarsministeriets normala styrning av Försvarsmakten. Försvarsministeriet styr också i fortsättningen Försvarsmakten samt den militära underrättelseinhämtningen som en del av Försvarsmakten genom ekonomi-, resurs- och budgetstyrning samt författningsstyrning.

Dessutom har försvarsministeriet en betydande roll vid övervakningen av förvaltningsområdet militär underrättelseinhämtning och behandlingen av den militära underrättelseinhämtningens årliga prioriteringar. Försvarsmakten lyder under försvarsministeriet i enlighet med 24 § i lagen om försvarsmakten.

Enligt 2 mom. i den föreslagna paragrafen underrättar försvarsministeriet också Försvarsmakten om de prioriteringar som behandlats förberedelsevis av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president. Det är fråga om en intern föreskrift för förvaltningsområdet genom vilken prioriteringarna fastställs. Efter det att försvarsministeriet har utfärdat föreskriften är Försvarsmakten skyldig att iaktta prioriteringarna.

I enlighet med de prioriteringar som behandlats förberedelsevis kan de myndigheter som avses i den paragraf som det föreskrivs om nedan lämna en begäran om information om en viss fråga till Huvudstaben. På basis av begäran om information utarbetar militärunderrättelsemyndigheterna mer detaljerade underrättelseuppdrag som kan utföras med användning av bl.a. metoder för underrättelseinhämtning.

I 3 mom. i den föreslagna paragrafen föreskrivs det om ledningen av den militära underrättelseinhämtningen som enligt paragrafen leds av Huvudstaben. Huvudstaben svarar i praktiken för ledningen av den militära underrättelseinhämtningen genom att mellan militärunderrättelsemyndigheterna dela upp de underrättelseuppdrag som de ska utföra. Bestämmelser om begäran om information finns nedan. Huvudstaben har också ansvar för att den militära underrättelseverksamheten och underrättelseuppdragen överensstämmer med de prioriteringar i underrättelseinhämtningen som den högsta statsledningen har fastställt.

Huvudstaben svarar i fråga om ledningen också för att den praktiska verksamhet som behövs vid underrättelseinhämtningen samordnas med den civila underrättelsemyndigheten och andra myndigheter.

**13 §.** *Begäran om information*. Enligt 1 mom. kan information om föremålen för den militära underrättelseinhämtningen begäras av Finlands utrikes- och säkerhetspolitiska högsta statsledning, vars behov av att få information tillgodoses genom den militära underrättelseinhämtningen. En begäran om information enligt paragrafen har samband med de föremål för militär underrättelseinhämtning som avses i 4 § i lagen och de prioriteringar som avses i 12 §.

I begäran om information ska myndigheten ge en så exakt beskrivning som möjligt av behovet av information samt beskriva hur behovet av information motsvarar de prioriteringar som har behandlats av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president.

Huvudstabens underrättelsechef ger på basis av en begäran om information ett underrättelseuppdrag till militärunderrättelsemyndigheten som närmare ska bestämma med vilka metoder för underrättelseinhämtning den behövliga informationen kan inhämtas på det mest ändamålsenliga sättet. Med stöd av den information som inhämtats utarbetar militärunderrättelsemyndigheten en utredning som överensstämmer med begäran om information och som Huvudstaben lämnar till den som begärt information.

Militärunderrättelsemyndigheten kan också till behövliga delar använda den rapport som utarbetats för att svara på begäran om information som grund för den utredning som ska utarbetas om den militära underrättelseverksamheten och lämnas till det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president.

Huvudstabens underrättelsechef fastställer på basis av begäran om information underrättelseuppdragen och militärunderrättelsemyndigheten fattar på basis av begäran beslut om vilka metoder för underrättelseinhämtning som ska användas för att inhämta informationen. Militärunderrättelsemyndigheten skaffar de i denna lag närmare angivna tillstånd och beslut som behövs för att befogenheterna ska kunna utövas. Det som nämns ovan bör dock inte blandas ihop med ett av en civil underrättelsemyndighet framlagt uppdrag om användning av underrättelseinhämtning som avser datatrafik, vilket det föreskrivs särskilt om nedan.

Den förvaltning som lyder under de myndigheter som räknas upp i paragrafen får inte på egen hand lägga fram en begäran om information utan den ska alltid gå via de myndigheter som

nämns i paragrafen. På så sätt säkerställs det att den förvaltning som lyder under myndigheterna inte använder en begäran om information för att kringgå sina egna befogenheter för att inhämta information om sina enskilda uppgifter. På detta sätt säkerställs det dessutom att en begäran om information också är tillräckligt viktig.

Avsikten med paragrafen är inte att påverka det normala myndighetssamarbetet och utbytet av information inom ramen för detta samarbete.

De militära kommandon som republikens president ger som Försvarsmaktens överbefälhavare ska åtskiljas från de begäranden om information som avses i paragrafen. Avsikten är inte att genom den lagstiftning som är under beredning ingripa i förfarandet för beslutsfattande om militära kommandon. Förfarandet i fråga om militära kommandon har behandlats i den allmänna motiveringen till denna proposition. Dessutom ska Försvarsmaktens interna behov av information, dvs. de underrättelseuppdrag som baserar sig på syftet med den militära underrättelseinhämtningen, åtskiljas från begärandena om information.

**14 §.** *Samordning av underrättelseverksamheten.* Enligt 1 mom. ska det genom samordningen av underrättelseinhämtningen säkerställas att man reagerar på sådana begäranden om information som har utrikes- och säkerhetspolitiska konsekvenser för underrättelseinhämtningen, beaktar synpunkterna hos de olika förvaltningsområden som har samband med underrättelseverksamheten samt informerar de behöriga aktörerna om det synsätt som man enats om vid denna process.

Funktionellt sett är det vid samordningen fråga om påvisande och koordinering av prioriteringarna i underrättelseinhämtningen samt fördelning av underrättelseverksamhetens uppgifter mellan den militära och den civila underrättelseinhämtningen på basis av en ändamålsenlighetsprövning av föremålen för underrättelseinhämtning och hotets art. I samband med denna prövning kan det göras en bedömning av t.ex. de utrikespolitiska dimensioner och konsekvenser som militär underrättelseinhämtning och civil underrättelseinhämtning som utförs annanstans än i Finland eventuellt har för Finlands internationella relationer.

Vid samordning av underrättelseverksamheten är det däremot inte fråga om övervakning av underrättelseinhämtningen eller styrning som inbegriper den operativa verksamheten, såsom beslut om användning av metoder för underrättelseinhämtning.

Enligt 1 mom. ska den militära och den civila underrättelseverksamheten samordnas mellan republikens president, statsrådets kansli, utrikesministeriet, försvarsministeriet och inrikesministeriet. Samordningen kan göras i samma sammansättning som i statsrådets samordningsgrupp för frågor som gäller lägesbilden. Till samordningsgruppen hör statssekreteraren vid statsrådets kansli, utrikesministeriets statssekreterare, inrikesministeriets och försvarsministeriets kanslichefer och kanslichefen vid republikens presidents kansli samt som sakkunniga-damöter chefen för skyddspolisen och Huvudstabens underrättelsechef. De aktörer som deltar i samordningen får behövligt administrativt stöd av de myndigheter som de representerar.

Vid samordningen av underrättelseinhämtningen preciseras vid behov de begäranden om information som lämnats till Huvudstaben.

Med stöd av 2 mom. i den föreslagna paragrafen kan begäranden om information som inbegriper utrikes- och säkerhetspolitiska konsekvenser samt utövande av befogenheter behandlas i styrande och samordnande syfte vid samordningen av underrättelseinhämtningen. Denna typ av ärenden kan vara i synnerhet sådana operationer för att inhämta information som förutsätter

särskilda befogenheter, eller operationer som kan anses vara utrikespolitiskt känsliga. Den samordning av underrättelseinhämtning som avses i momentet inbegriper inte ärenden som gäller övervakning och inte heller operativt beslutsfattande, utan vid samordningen ska beaktas t.ex. olika förvaltningsområdens ståndpunkter i situationer där underrättelseverksamhet t.ex. kan skada eller ha andra konsekvenser för Finlands internationella relationer.

Vid samordningen av underrättelseinhämtning kan det också från fall till fall göras en granskning av de befogenheter som ska utövas för att genomföra en begäran om information och en bedömning av de politiska riskerna med utövandet av befogenheterna. De ärenden som behandlas vid samordningen är inte begäranden om information eller underrättelseuppdrag som kan anses vara vanliga.

Samordningen av underrättelseinhämtning säkerställer också att informationen lämnas till de behöriga aktörerna t.ex. när det gäller underrättelseinhämtning som avser utländska förhållanden. Vid samordningen kan den behöriga myndigheten dock få information som är viktig med tanke på dess verksamhet samt stöd för sitt operativa beslutsfattande.

De underrättelseärenden som avgörs som militära kommandomål behöver inte samordnas, utan de betraktas direkt som militära kommandon. Avsikten med lagen om militär underrättelseverksamhet är inte att ändra förfarandet för beslutsfattande om militära kommandomål.

**15 §.** *Tillsynen över den militära underrättelseinhämtningen.* Enligt 1 mom. är försvarsministeriet skyldigt att minst en gång per år ge det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president en redogörelse för den informationsinhämtning som gjorts på basis av prioriteringarna i underrättelseinhämtningen till den del som informationsinhämtningen hör till militärunderrättelsemyndighetens ansvarsområde.

Om den information som inhämtats om föremålen för underrättelseinhämtning enligt prioriteringarna förutsätter det kan en redogörelse ges också oftare på begäran av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president eller på försvarsministeriets eget initiativ. I de senare situationerna kan det vara fråga om t.ex. information som har betydelse för skötseln av Finlands utrikespolitik eller för Finlands internationella relationer.

I den redogörelse som ska lämnas är det inte fråga om laglighetsövervakning utan om resultaten av den informationsinhämtning som inletts på basis av de prioriteringar som har behandlats förberedelsevis av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president. Redogörelsen kan innehålla en genomgång av t.ex. säkerhetsläget i Finland och de faktorer som påverka det, om detta avses i prioriteringarna. På så sätt säkerställs det att den högsta statsledningen har kännedom om den säkerhetspolitiska miljön i Finland och om förändringarna i den.

Enligt 2 mom. är Huvudstaben skyldig att årligen eller på begäran av försvarsministeriet ge försvarsministeriet en redogörelse för underrättelseverksamheten. Bestämmelsen är viktig med tanke på den allmänna styrningen av försvarsministeriets förvaltningsområde, uppföljningen av resultaten och tillsynen över lagenligheten.

Den redogörelse som lämnas till försvarsministeriet ska vara mer omfattande än den redogörelse som lämnas till det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president. Av redogörelsen ska framgå alla underrättelseuppdrag som utförts med stöd av de prioriteringar som har behandlats förberedelsevis av det gemen-

samma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president samt de svar på olika myndigheters begäranden om information som getts med stöd av prioriteringarna.

Vid den uppföljning som utförs av försvarsministeriet och avses i momentet är det inte fråga om laglighetsövervakning, som det föreskrivs om nedan.

3 kap. **Samverkan med andra myndigheter och internationellt samarbete**

**16 §.** *Samarbete med skyddspolisen.* De ökande riskerna och nya typerna av hot förutsätter kontinuerlig beredskap och förberedelser av hela samhället. Dessutom stärks det övergripande säkerhetstänkandet nationellt samt inom EU och i det internationella samarbetet.

Det är inte nödvändigtvis självklart att militära hot eller hot mot Finlands nationella säkerhet utgör primära föremål för inhämtande av information inom den militära eller den civila underrättelseinhämtningen. Hoten kan till sin art vara sådana att de med tiden och i takt med att händelsekedjorna framskrider kan utgöra t.ex. militära hot. Underrättelsemyndigheterna ska smidigt kunna utbyta information och överföra ett underrättelseuppdrag till en annan underrättelsemyndighet, om det visar sig att föremålet för inhämtande av information snarare är ett föremål för civil underrättelseinhämtning än militär underrättelseinhämtning.

Enligt paragrafen ska en militärunderrättelsemyndighet agera i samarbete med skyddspolisen för att underrättelsemyndigheternas uppgifter ska kunna skötas på ett ändamålsenligt sätt och i detta syfte, trots vad som föreskrivs om sekretess, ge skyddspolisen behövliga uppgifter.

I 10 § i förvaltningslagen (434/2003) finns det en allmän bestämmelse om samarbete mellan myndigheterna och deras skyldighet att sträva efter att främja samarbetet mellan myndigheterna, vilket preciseras genom den bestämmelse som behandlas i denna proposition. För att målen med informationsinhämtningen ska uppnås och informationsinhämtningen ska kunna inriktas på ett exakt och ändamålsenligt sätt förutsätts det att underrättelsemyndigheterna samarbetar. Dessutom främjar samarbete att gemensamma förfaranden och praxis utformas.

Det samarbete som avses i förvaltningslagen omfattar inte rätt att lämna ut sekretessbelagda uppgifter mellan myndigheterna, och därför föreskrivs det i slutet på paragrafen uttryckligen om utlämnande av dessa uppgifter mellan militärunderrättelsemyndigheterna och skyddspolisen.

Genom samarbetet mellan myndigheterna säkerställs det också att militärunderrättelsemyndigheten och civil underrättelsemyndigheten är tillräckligt medvetna om den informationsinhämtning som utförs av den andra parten så att t.ex. underrättelseoperationer inte äventyras eller hindras på grund av en annan myndighets verksamhet. Dessutom kan det med tanke på myndigheternas resurser inte anses ändamålsenligt att underrättelsemyndigheterna inte kan dela sin materiel och sitt kunnande med en annan underrättelsemyndighet.

Vid samarbetet ska det dock särskilt beaktas att underrättelseinhämtningen hålls åtskild från verksamhet som avser utredning av brott. Ändamålet med och förutsättningarna för dessa befogenheter avviker i betydande grad från varandra. I 76 och 77 § föreskrivs det på ett heltäckande sätt om utlämnande av uppgifter för förundersökning och brottsbekämpning.

Genom paragrafen regleras inte behandlingen och utlämnandet av personuppgifter utan mer allmänt förutsättningarna för samarbete. I lagen om behandling av personuppgifter inom För-

svarsmakten föreskrivs det i enlighet med hänvisningen i 2 § i denna lag särskilt om utlämnande av personuppgifter.

**17 §.** *Samarbete med andra myndigheter och sammanslutningar.* Enligt 1 mom. ska militärunderrättelsemyndigheterna enligt behov agera i samarbete med andra myndigheter för att den militära underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt.

Att samarbetet mellan myndigheterna fungerar har en central betydelse för att målen med den militära underrättelseinhämtningen ska kunna uppnås. Samarbetet omfattar utvecklande av datasystem, skapande av en lägesbild över säkerhetshot och förändringar i verksamhetsmiljön, gemensamma handlingsplaner, ömsesidig handräckning samt utbildningssamarbete.

Det är också fråga om den taktiska verksamhet mellan myndigheter som sker inom ramen för andra myndigheters normala uppgifter och som inte gäller användning av metoder för underrättelseinhämtning. Viktiga myndigheter med tanke på militärunderrättelsemyndigheten är i synnerhet gränsbevakningsväsendet och Tullen. Det kan vara fråga om att med stöd av praktiska arrangemang t.ex. förhindra att en täckoperation eller informationskälla avslöjas.

Enligt 2 mom. kan militärunderrättelsemyndigheterna för att genomföra sitt uppdrag agera i samarbete med sammanslutningar samt till andra myndigheter och sammanslutningar trots sekretessbestämmelserna lämna ut uppgifter, om utlämnandet av uppgifterna är nödvändigt med avseende på försvaret av landet eller för att skydda den nationella säkerheten.

I samband med militär underrättelseinhämtning kan det uppkomma situationer där det för att skydda försvaret av landet eller den nationella säkerheten är behövligt att på eget initiativ eller på begäran lämna ut information till en annan myndighet. Detsamma gäller i övrigt utlämnande av information till en annan myndighet för att den ska kunna sköta sina uppgifter. Det är fråga om utlämnande av andra uppgifter än sådana uppgifter som avses i lagen om behandling av personuppgifter inom Försvarsmakten, vilket det föreskrivs om i den lagen.

I de situationer som avses i momentet ska utlämnandet av information höra till syftet med den militära underrättelseinhämtningen enligt 3 § i denna lag. Militärunderrättelsemyndigheten ska göra en inledande prövning av utlämnandet av information i anslutning till sitt eget uppgiftsområde. Utlämnandet av uppgifter ska dessutom vara nödvändigt. På så sätt betonas det att tröskeln för att lämna ut uppgifter ska vara hög. Uppgifter får inte lämnas ut i några andra fall än de fall som uppfyller de förutsättningar som anges i momentet.

Samarbetet mellan militärunderrättelsemyndigheten och sammanslutningar kan också ha samband med ett företags säkerhet och förhindrande av företagsspionerі. I dessa situationer ska särskild uppmärksamhet också fästas vid vilken ställning ett företag har när det gäller försvaret och om företaget t.ex. deltar i upprätthållandet av samhällets vitala funktioner.

I 3 mom. finns en hänvisningsbestämmelse till 76 och 77 § där det föreskrivs om utlämnande av information till centralkriminalpolisen i vissa fall.

**18 §.** *Samordning av hemlig informationsinhämtning.* I paragrafen föreskrivs det om samordningen av hemlig informationsinhämtning mellan militärunderrättelsemyndigheten, skyddspolisen, centralkriminalpolisen och en annan myndighet. Det är fråga om en specialbestämmelse i förhållande till de bestämmelser om samarbete som föreslås ovan.

I synnerhet överlappande operationer som utförs av myndigheter som utför hemligt inhämtande av information och av militärunderrättelsemyndigheterna kan utgöra en allvarlig arbetssäkerhetsrisk, om myndigheterna agerar utan kännedom om varandra.

När det finns flera myndigheter som har rätt att använda hemlig informationsinhämtning kan detta i vissa fall medföra en risk för att både säkerhetsmyndigheternas roller och enskilda operationer överlappar. För att det ska gå att på förhand förhindra denna typ av situationer och förhindra eventuella olycksfall i arbetet kan det från fall till fall vara nödvändigt att dessa myndigheter sinsemellan samordnar användningen av hemlig informationsinhämtning.

**19 §.** *Internationellt samarbete.* I paragrafen föreskrivs det om militärunderrättelsemyndigheternas internationella samarbete. Med samarbete avses allt internationellt samarbete mellan underrättelse- och säkerhetsmyndigheter samt samarbete mellan militärunderrättelsemyndigheterna och andra länders motsvarande organ. Paragrafen gäller inte det utbyte av personuppgifter som det föreskrivs särskilt om, utan det är fråga om annat samarbete, såsom operativt samarbete och t.ex. utbildningssamarbete. Med internationellt samarbete avses t.ex. utbyte av information, givande av tekniskt stöd, utbildningssamarbete, tjänstemannautbyte och internationell kontaktpersonverksamhet. Med gemensamma underrättelseoperationer avses gemensamt inhämtande av information där de metoder för underrättelseinhämtning som avses i 4 kap. i denna lag används. Internationellt samarbete ska alltid överensstämma med Finlands nationella intressen.

Inom området för underrättelseinhämtning gäller inga internationella juridiskt bindande konventioner. Stater, inklusive Finland, har ingått arrangemang som tangerar ämnet, men som högst kan anses vara samförståndsprotokoll och som varken är folkrättsligt bindande eller förpliktande. En orsak till detta är det primära syftet med underrättelseverksamheten, vilket är att främja det egna landets nationella intressen. Detta betyder dock inte att ett nationellt intresse inte kan överensstämma med andra staters nationella intressen och bäst uppnås genom samarbete mellan olika staters underrättelsemyndigheter.

Militärunderrättelsemyndigheten ska också i det internationella samarbetet beakta de allmänna principerna för militär underrättelseverksamhet samt Europakonventionen och lagstiftningen i Europeiska unionen och Finland.

Europeiska unionens behörighet gäller inte den nationella säkerheten. Trots detta ska man när t.ex. personuppgifter lämnas ut till i synnerhet stater utanför Europeiska unionen beakta Europeiska unionens rättsakter om dataskydd samt rättspraxis vid Europeiska unionens domstol i den utsträckning som krävs. Europeiska unionens domstol har bl.a. ansett att allmän överföring av personuppgifter kränker det centrala innehållet i den grundläggande rättigheten som gäller respekten för privatlivet, om de nationella bestämmelserna i den stat som tar emot personuppgifterna möjliggör att myndigheterna har allmän tillgång till innehållet i elektronisk kommunikation utan att myndigheternas rätt att använda eller bevara personuppgifter är begränsad, och om de nationella bestämmelserna i den mottagande staten inte möjliggör att individer utnyttjar rättsmedel i egen sak. Bestämmelser om behandling av personuppgifter inom Försvarsmakten finns i lagen om behandling av personuppgifter inom Försvarsmakten.

Avsikten med det internationella samarbete som avses i paragrafen är inte att ingripa t.ex. i försvarsgrenarnas internationella samarbete, vars författningsgrund finns i 42 § i territorialövervakningslagen. Försvarsgrenarna får för skötseln av sina uppgifter information om t.ex. de krigsfartyg som används av en annan stat, vilket kan vara intressant information för en utländsk samarbetspart också med tanke på denna stats underrättelsemyndigheter. Den informat-

ion som utbyts kan i detta avseende dock inte betraktas som underrättelseinformation, utan information utbyts som en del av territorialövervakningssamarbetet. Om de befogenheter som avses i denna lag behövs för att inhämta information, ska informationen behandlas och utbytas i enlighet med denna lag.

Enligt 1 mom. i den föreslagna paragrafen kan militärunderrättelsemyndigheterna i enlighet med Finlands nationella intressen i anknytning till sina uppgifter delta i internationellt samarbete. Hot mot den militära underrättelseinhämtningens uppgifter är ofta internationella till sin karaktär och därför har utländska underrättelsetjänster och säkerhetstjänster möjlighet att få information om dessa hot.

Med nationella intressen avses att internationellt samarbete har bedömts ligga i Finlands intressen och inte medföra att de olika delområdena i det finska samhället försvagas. Det ligger t.ex. inte i Finlands nationella intressen att ett visst finskt företags företagshemligheter utlämnas till militärunderrättelsemyndighetens utländska samarbetsparter. Vid bedömningen av Finlands nationella intressen ska uppmärksamhet också fästas vid människorättssituationen i den mottagande eller utlämnande staten och hur denna stat iakttar internationella konventioner om mänskliga rättigheter. De sistnämnda aspekterna ska beaktas i prövningen till följd av de bestämmelser som förpliktar militärunderrättelsemyndighetens tjänstemän, såsom grundlagen och förvaltningslagen samt de allmänna principer som föreslås i denna proposition.

Enligt 1 punkten i momentet kan militärunderrättelsemyndigheterna utbyta underrättelseuppgifter med utländska underrättelsetjänster och säkerhetsmyndigheter. De uppgifter som militärunderrättelsemyndigheterna inhämtat kan utöver för tryggandet av Finlands försvar och den nationella säkerheten ha stor betydelse internationellt t.ex. med tanke på utvecklingen av militära hot och kriser. När uppgifter lämnas ut ska bestämmelserna om behandling av personuppgifter samt internationella avtal om utlämnande av uppgifter och därmed ansluten rättspraxis alltid tas i beaktande.

Militärunderrättelsemyndigheterna har endast rätt att lämna ut sådan information som den innehar i enlighet med sina uppgifter. Den information som lämnas ut ska alltid ha samband med de föremål för militär underrättelseinhämtning och hot som avses i 4 §. Den information som lämnas ut får inte vara överflödig information eller annan information som genererats vid inhämtandet av information och som militärunderrättelsemyndigheterna inte egentligen haft rätt att inhämta eller använda, utan militärunderrättelsemyndigheterna ska också själva kunna använda informationen för sina egna syften. Utbyte av information kan gälla t.ex. en främmande stats vapenindustri.

Militärunderrättelsemyndigheterna kan av utländska underrättelsetjänster och säkerhetsmyndigheter ta emot information som gäller myndighetens uppgifter. Hot mot den militära underrättelseinhämtningens uppgifter är ofta till sin art internationella och också utländska underrättelse- och säkerhetstjänster har möjlighet att få sådan information om dessa hot som militärunderrättelsemyndigheten inte har kunnat få med stöd av sina egna befogenheter. Dessutom är det särskilt när det gäller personbaserad underrättelseinhämtning fråga om en långvarig och planmässig verksamhet som en militärunderrättelsemyndighet ännu inte har haft möjligheter till eller ännu inte har erfarenhet av. Militärunderrättelsemyndigheterna kan med stöd av det internationella samarbetet t.ex. få viktig information som behövs för att myndigheten ska kunna inleda sin egen personbaserade underrättelseinhämtning som avser utländska förhållanden eller börja utöva någon annan befogenhet.

Det kan också vara fråga om teknik och taktik som gäller metoder för underrättelseinhämtning, information om sabotageprogram eller analyser av säkerhetshot eller annan sådan information som det ligger i Finlands intressen att lämna ut. Utlämnande av information ska dock alltid ligga i det nationella intresset. Detta intresse omfattar t.ex. information om Finlands politiska eller ekonomiska relationer med en annan stat, information om den militära eller den civila underrättelseinhämtningen eller det militära försvaret eller information för att trygga det internationella underrättelsesamarbetet.

De situationer som avses i punkten kan vara t.ex. den underrättelseinhämtning som utförs i internationella militära krishanteringsinsatser i fråga om hot som riktar sig mot operationer, men information som är viktig för beslut om deltagande i en insats kan också fås med hjälp av det internationella samarbetet.

Den information som lämnas ut ska bedömas som en helhet utifrån de ovan nämnda aspekterna och vid bedömningen ska beaktas också egenskaperna hos den information som lämnas ut samt den aktör som tar emot informationen.

Det internationella samarbetet i fråga om underrättelseverksamhet är alltid förenat med osäkerhet när det gäller hur tillförlitlig den information som utbyts är. Kvaliteten på de uppgifter som militärunderrättelsemyndigheterna lämnar ut och på uppgifter om en viss person ska alltid verifieras och uppgifterna ska, om möjligt, förses med information som gör det möjligt för mottagaren att bedöma hur korrekta, fullständiga, aktuella och tillförlitliga uppgifterna är. Om det framgår att t.ex. felaktiga personuppgifter har lämnats ut eller att uppgifter har lämnats ut på ett lagstridigt sätt, ska mottagaren utan dröjsmål meddelas om detta. En bedömning av uppgifternas tillförlitlighet ska göras redan när de inhämtade uppgifterna analyseras.

Det kan anses höra till underrättelseverksamhetens grundkaraktär att den inbegriper osäkerhetsfaktorer, inexaktheter och mångtydighet. Detta betyder dock inte att informationen inte får användas, utan att militärunderrättelsemyndigheterna i fråga om i synnerhet uppgifter som gäller personer enligt behov ska säkerställa att uppgifterna faktiskt är korrekta genom att t.ex. inleda en underrättelseoperation.

Enligt 2 punkten i momentet kan militärunderrättelsemyndigheterna delta i internationellt samarbete i anknytning till inhämtande och bedömning av underrättelseuppgifter. I 4 § nämns som vissa föremål för den militära underrättelseinhämtningen också internationella insatser och händelser. De finska militärunderrättelsemyndigheterna kan som en del av dessa delta i internationellt samarbete som baserar sig på det internationella bistånd som en EU-medlemsstat begär med stöd av ett grundfördrag.

I 2 mom. i den föreslagna paragrafen föreskrivs det om situationer där tjänstemän vid militärunderrättelsemyndigheterna på en annan stats territorium deltar i samarbetet mellan militärunderrättelsemyndigheterna och en utländsk underrättelse- eller säkerhetsmyndighet. Om gemensam informationsinhämtning genomförs i samarbete med den stat på vars territorium metoder för underrättelseinhämtning är avsedda att användas, ska militärunderrättelsemyndigheternas tjänstemän iaktta de begränsningar och villkor för verksamheten som staten i fråga ställer. Militärunderrättelsemyndigheternas tjänstemän kan när de deltar i samarbetet i en annan stat i detta fall med den statens samtycke använda de metoder för underrättelseinhämtning som avses i 4 kap. eller motsvarande metoder. Metoder för underrättelseinhämtning kan i detta fall användas endast i den utsträckning och på det sätt som staten i fråga tillåter. Bestämmelsen gäller alltså samarbetet med territorialstaten i fråga. Uttrycket ”i samarbete med” kan anses täcka också sådant samarbete som baserar sig på en territorialstats samtycke och som

territorialstaten inte själv deltar i. Om samarbetet däremot utförs på en tredjestats territorium så ska på de metoder för underrättelseinhämtning som militärunderrättelsemyndigheten använder tillämpas det som föreskrivs om underrättelseinhämtning som avser utländska förhållanden.

En militärunderrättelsemyndighets tjänsteman är också vid samarbete utomlands underställd militärunderrättelsemyndighetens styrning samt intern och extern tillsyn, och tjänstemannen har samma rättigheter och skyldigheter som i annan underrättelseinhämtning som avser utländska förhållanden.

I 3 mom. fastställs det att en behörig tjänsteman från en främmande stat med ett beslut av Huvudstabens underrättelsechef har rätt att på finskt territorium för skötsel av militärunderrättelsemyndigheternas uppgifter eller tryggande av Finlands nationella säkerhet samarbeta med en tjänsteman vid en militärunderrättelsemyndighet samt under dennes uppsikt och övervakning använda de metoder för underrättelseinhämtning som avses i 20, 22, 41, 45, 49 och 63 §.

Till skillnad från 2 mom. tillåts det med stöd av detta moment att en tjänsteman från en annan stat deltar i samarbete på finskt territorium. I samarbetet ska en tjänsteman från en främmande stat handla på Finlands ansvar, under Finlands uppsikt och ledning samt i enlighet med den finska lagstiftningen. När en tjänsteman från en främmande stat är verksam i Finland ska tjänstemannen följa de anvisningar som militärunderrättelsemyndigheten ger honom eller henne och de begränsningar som militärunderrättelsemyndigheten ställer för honom eller henne.

Dessa metoder för underrättelseinhämtning innebär endast ett litet ingripande i de grundläggande fri- och rättigheterna och ingen av metoderna inkräktar på hemligheten i fråga om förtroliga meddelanden. En tjänsteman från en främmande stat kan använda dessa metoder för underrättelseinhämtning under uppsikt och övervakning av en tjänsteman vid militärunderrättelsemyndigheten, vilket innebär att militärunderrättelsemyndigheten ansvarar för den gemensamma operationen och de metoder för underrättelseinhämtning som används inom ramen för denna operation. Systematisk observation kan utföras både i den reella världen och i datanät. I synnerhet vid observation av datanät kan det behövas hjälp av en sådan tjänsteman från en annan stat som har en egenskap eller ett kunnande som tjänstemännen vid militärunderrättelsemyndigheten inte har, såsom språkkunskaper eller kunskaper om kultur. Ett motsvarande behov av samarbete kan uppkomma i anslutning till täckoperationer, bevisprovokation genom köp eller styrd användning av informationskällor. Det är fråga om att en tjänsteman från en främmande stat har en biträdande roll i militärunderrättelsemyndighetens informationsinhämtningsoperation. En utländsk tjänsteman kan ha ett kunnande eller andra färdigheter som en finsk tjänsteman inte har och som behövs för att ett underrättelseuppdrag ska kunna utföras framgångsrikt.

Enligt 4 mom. fattas beslutar Huvudstabens underrättelsechef om deltagande i internationellt samarbete.

Ett beslut om deltagande i samarbete ska basera sig på syftet med den militära underrättelseinhämtningen eller tryggande av Finlands nationella säkerhet. Om verksamheten baserar sig på tryggande av den nationella säkerheten i samarbete med t.ex. en annan stat på den statens territorium ska samarbetet åtminstone indirekt tangera tryggande av Finlands nationella säkerhet. En sådan situation kan uppkomma t.ex. när det är behövligt att få information om den verk-

samhet som en aktör som är verksam på den andra statens territorium bedriver och det kan antas att denna verksamhet påverkar eller kommer att påverka Finlands nationella säkerhet.

Också beslut om att en tjänsteman från en främmande stat kan använda vissa metoder för underrättelseinhämtning som det föreskrivs särskilt om i denna paragraf ska fattas av Huvudstabens underrättelsechef. En tjänsteman från en främmande stat kan delta i samarbete i Finland endast när det är tillåtet enligt lagstiftningen i den stat som sänder ut tjänstemannen.

I fråga om beslutsfattande om det internationella samarbete som avses i paragrafen ska det som föreskrivs i lagen om beslutsfattande om lämnande av och begäran om internationellt bistånd (418/2017) också beaktas.

I 5 mom. avses med internationella förpliktelser främst internationella fördrag som gäller informationssäkerhet och som Finland redan har ingått med flera betydande samarbetsparter.

Dessutom finns det i bestämmelsen en hänvisning till lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004), som har företräde i förhållande till lagen om offentlighet i myndigheternas verksamhet (621/1999). Den lag som nämns ovan tillämpas på utländska säkerhetsklassificerade uppgifter som ska skyddas med stöd av internationella överenskommelser om informationssäkerhet. I momentet finns också en informativ hänvisning till lagen om behandling av personuppgifter inom Försvarsmakten.

4 kap. **Metoder för underrättelseinhämtning**

I kapitlet föreskrivs det om sådana allmänna befogenheter till informationsinhämtning som är av samma typ som polisens och Försvarsmaktens gällande befogenheter till informationsinhämtning för att förebygga brott.

Utöver de befogenheter som föreskrivs i kapitlet har militärunderrättelsemyndigheten också tillgång till sådana metoder för inhämtande av information som kan användas utan särskilda bestämmelser om befogenheter. Dessa metoder är underrättelseinhämtning ur öppna källor, bildunderrättelser och geografisk underrättelseinhämtning. Det är fråga om informationsinhämtning som inte kan anses kränka skyddet för privatlivet. Underrättelseinhämtning ur öppna källor kan inte anses vara en myndighetsverksamhet som enligt grundlagen ska regleras genom lag.

Med underrättelseinhämtning ur öppna källor avses bl.a. militärunderrättelsemyndighetens inhämtande av information ur offentliga medier, offentliga myndighetsregister, offentligt tillgängliga databaser samt uttalanden som har framförts i offentligheten. Information ur öppna källor består av uppgifter som varje enskild person har laglig tillgång till t.ex. på begäran eller genom att själv göra observationer. Typiska informationskällor är litteratur, statistik, kartor, tidningar, publikationer, televisions- och radiosändningar riktade till allmänheten samt myndigheter och sociala medier. Vid underrättelseinhämtning ur öppna källor uppfattas internet inte som en egen informationskälla, utan som en kanal via vilken information inhämtas. Underrättelseinhämtning ur öppna källor kan delas in i inhämtande av information samt mediebevakning vars huvudsakliga syfte är att stödja att det skapas en lägesbild för underrättelseinhämtningen.

Underrättelseinhämtning ur öppna källor används som stöd för andra metoder för inhämtande av information eller som en fristående metod för underrättelseinhämtning. Kännetecknande för inhämtande av information ur öppna källor är den stora mängden information samt möjlig-

heten till desinformation. Till fördelarna med denna typ av informationsinhämtning hör däremot att den är snabb, billig och geografiskt obegränsad samt att information kan samlas in om kommande händelser. Underrättelseinformation som baserar sig endast på öppna källor har en lägre skyddsnivå än annan underrättelseinformation, varvid också sätten att använda information är mångsidigare.

I samband med bildunderrättelser kan militärunderrättelsemyndigheten t.ex. med elektrooptiska metoder och radarbilder inhämta information om ett område, utvecklingen av området och den verksamhet som bedrivs på området. Bildunderrättelser innebär att inhämta information för att kunna skapa en lägesbild på strategisk nivå, dvs. det är inte fråga om inhämtande av information om en enskild individ. Information inhämtas om stora områden och utvecklingen av dem och denna utveckling kan ha betydelse med tanke på Försvarsmaktens verksamhet, såsom förändringar i placeringen av en främmande stats trupper.

Bildunderrättelser är nödvändiga för att oberoende och självständigt kunna bedöma bl.a. säkerhetspolitiskt betydande händelser. Den information som militärunderrättelsemyndigheten inhämtat på detta sätt stöder direkt Finlands utrikespolitik bl.a. när det gäller vilka stater som sprider massförstörelsevapen. Bildunderrättelser kan användas också t.ex. för att trygga säkerheten för finska krishanteringsstyrkor (egenskydd, dvs. force protection). Med bildunderrättelser inhämtas inte information om enskilda personer och bildunderrättelser kan inte riktas mot ärenden som omfattas av skyddet för privatlivet.

Med geografisk underrättelseinhämtning kan militärunderrättelsemyndigheten få en mer omfattande bild av t.ex. en främmande stats geografiska förhållanden och verksamhetsmiljön i ett område. Syftet med geografisk underrättelseinhämtning är att beskriva, bedöma och presentera vissa objekt, områden, naturfenomen och förhållanden. Vid geografisk underrättelseinhämtning utnyttjas bl.a. nationellt och internationellt geografiskt informationsmaterial och bildmaterial, uppgifter om förhållanden samt statistiska uppgifter. Militärunderrättelsemyndigheten kan även beställa sådan information av utomstående aktörer som stöd för sin egen underrättelseinhämtning.

Militärunderrättelsemyndigheten får utöver genom de metoder för inhämtande av information som avses ovan också den information som behövs för underrättelseinhämtningen av t.ex. Försvarsmaktens andra enheter. Framtagande av denna typ av information utgör en del av Försvarsmaktens normala verksamhet. Information som behövs för militär underrättelseinhämtning kan vara ett resultat av t.ex. Försvarshögskolans forskning eller territorialövervakningen. Dessutom kan information fås via myndighetssamarbete.

Med personbaserad underrättelseinhämtning avses informationsinhämtning som baserar sig på personkontakt eller personligt iakttagande av en person eller ett annat objekt. Personbaserad underrättelseinhämtning kan utföras t.ex. med hjälp av sociala medier. Vid personbaserad underrättelseinhämtning inriktas informationsinhämtningen på människor och de dokument och elektroniska upptagningar som de innehar, och på grund av detta ska det uttryckligen i lag finnas bestämmelser om den personbaserade underrättelseinhämtningens befogenheter.

Med hjälp av personbaserad underrättelseinhämtning kan man inhämta viktig information om den säkerhetspolitiska miljön och om exempelvis väpnade styrkors, underrättelsetjänsters, enskilda personers eller organisationers verksamhet och om de frågor med anknytning till Finlands försvar som är föremål för dessa aktörers intresse. Informationen kan gälla också t.ex. dokument, planer, den allmänna sinnesstämningen eller relationerna mellan personer. Personbaserad underrättelseinhämtning kan med stöd av de befogenheter som fastställs i detta kapitel

gälla också utländska aktörer i Finland vid sidan av den verksamhet som bedrivs utomlands. Den personbaserade underrättelseinhämtningens befogenheter till informationsinhämtning är t.ex. systematisk observation, teknisk observation och användning av informationskällor. Genom personbaserad underrättelseinhämtning kan det tas fram sådan detaljerad och mångsidig information av högsta skyddsnivå som det är svårt eller omöjligt att inhämta med andra typer av underrättelseinhämtning. Med hjälp av personbaserad underrättelseinhämtning kan det skapas förutsättningar för att effektivt utnyttja också andra typer av underrättelseinhämtning.

Med den personbaserade underrättelseinhämtningens metoder för inhämtande av information försöker man aktivt inhämta information om t.ex. väpnade styrkors, underrättelsetjänsters, enskilda personers eller organisationers verksamhet och om de frågor med anknytning till Finlands försvar som är föremål för dessa aktörers intresse.

De befogenheter till underrättelseinhämtning som utövas vid personbaserad underrättelseinhämtning motsvarar till många delar de befogenheter till hemligt inhämtande av information som anges i 5 kap. i polislagen och som också Försvarsmakten i nuläget redan delvis utövar. I princip föreskrivs det i 5 kap. i den gällande polislagen uttömmande om metoder för inhämtande av information, vilket innebär att de befogenheter som tidigare etablerats i riksdagsbehandlingen inte behöver ändras i fråga om underrättelseinhämtningen. I fråga om bestämmelserna om befogenheter är dessutom grundlagsutskottets tolkningspraxis etablerad och omfattande och bestämmelserna har utarbetats med grundlagsutskottets medverkan.

Trots att befogenheterna de facto motsvarar de befogenheter som anges i 5 kap. i polislagen avviker de från det kapitlet vad gäller skrivsättet och utövandet. Trösklarna för utövande är desamma när befogenheterna anpassas till underrättelseverksamheten.

Med avvikelse från 5 kap. i polislagen har det i bestämmelserna om befogenheter i det 4 kap. som föreslås i denna proposition tagits in särskilda förutsättningar för och särskilda förbud mot utövande av en befogenhet, såsom förbud mot att rikta informationsinhämtning mot ett utrymme som används för stadigvarande boende. Syftet med denna författningstekniska lösning är att förtydliga regleringen av befogenheter så att regleringen av utövandet av en befogenhet har tagits in direkt i bestämmelsen om befogenheten samt i bestämmelsen om beslut om utövande av befogenheten.

Eftersom det vid underrättelseverksamhet inte är fråga om förebyggande och bekämpning av brott har hänvisningar till brott inte tagits in i bestämmelserna om befogenheter. I bestämmelserna om befogenheter har det endast inkluderats sådant som är väsentligt med tanke på behovet av underrättelseinhämtning.

Den ordning som bestämmelserna om befogenheter presenteras i avviker från det som föreskrivs i 5 kap. i polislagen. Bestämmelserna om befogenheter är ordnade så att de börjar med de befogenheter som ingriper minst i de grundläggande fri- och rättigheterna och framskrider mot de befogenheter som mest ingriper i de grundläggande fri- och rättigheterna och hemligheten i fråga om förtroliga meddelanden. I slutet av kapitlet finns befogenheter som i nuläget inte har några motsvarigheter i lagstiftningen.

Det är med tanke på utvecklingen av Försvarsmaktens kapacitet viktigt att för att kunna utveckla Försvarsmaktens egen kapacitet få information om t.ex. vilka intentioner och planer staterna i närområdena har. Det kan vara fråga om information som inte är tillgänglig ur vanliga dokument eller meddelanden utan endast ur t.ex. diskussioner som förs mellan människor och som endast den andra part som deltagit i diskussionen kan lämna information om. Vid in-

hämtandet av sådan information har användningen av medhjälpare och det ovillkorliga fulla förtroende som hör ihop med denna användning en mycket viktig roll.

Med befogenheterna att inhämta information genom personbaserad underrättelseinhämtning strävar man utöver till informationsinhämtning också till att på ett tillräckligt tryggt och tillförlitligt sätt skydda och säkerställa underrättelseverksamheten. För att t.ex. garantera en informationskällas säkerhet är det inte i alla situationer ändamålsenligt att framträda som en underrättelsemyndighet och för att trygga ett underrättelseuppdrag är det inte heller i alla situationer ändamålsenligt att ta kontakt med en eventuell informationskälla, vilket innebär att det i dessa situationer kan vara ändamålsenligt att använda en täckoperation. Militärunderrättelsemyndigheten kan med stöd av befogenheterna till personbaserad underrättelseinhämtning också försäkra sig t.ex. om att en person som frivilligt hjälper militärmyndigheten faktiskt är frivillig för uppgiften samt säkerställa andra eventuella bakomliggande motiv.

Personbaserad underrättelseinhämtning kan ske både på Finlands territorium och utanför Finlands gränser. Personbaserad underrättelseinhämtning inriktar sig uttryckligen på utländska mål och förhållanden, också sådana mål som finns på Finlands territorium. Avsikten är att skapa en lägesbild och som stöd för kapaciteten inhämta nödvändig information utifrån vilken den högsta statsledningen får nödvändig information till stöd för sitt utrikes-, säkerhets- och försvarspolitiska beslutsfattande.

Till följd av karaktären hos den personbaserade underrättelseinhämtning som sker utomlands är den allmänna utgångspunkten med verksamheten att den behövliga informationen ska inhämtas med den enklast möjliga metoden. I praktiken baserar sig underrättelseinhämtning ofta på verksamhetsmodeller som påminner mycket om samarbete. Det är fråga om ett sådant utbyte av information och synpunkter mellan myndigheterna i två stater som baserar sig på frivillighet och som gagnar båda parterna. Informationsutbytet kan gälla t.ex. företeelser som är föremål för ett gemensamt intresse, enskilda händelser, observationer eller politiska stämningar och som den part som ger information erbjuder sin egen tolkning av och på så sätt försöker påverka den mottagande partens åsikter. Utöver denna typ av ömsesidigt informationsutbyte kan underrättelseverksamhet som avser utländska förhållanden också basera sig på endast den verksamhet som utförs av den stat som bedriver underrättelseinhämtning.

I grundläget inbegriper verksamheten att den personal som den stat som bedriver underrättelseinhämtning skickar utomlands med stöd av sin tjänsteställning gör allmänna observationer om förhållandena i staten de är stationerade i samt för diskussioner med representanter för eller medborgare i den staten. Trots att det i detta fall inte är fråga om ett informationsutbyte som det uttryckligen avtalats om med stationeringsstaten sker verksamheten oftast med stöd av stationeringsstatens tysta godkännande. Alla stater är de facto tvungna att upp till en viss gräns tolerera underrättelseinhämtning på sitt territorium.

Personbaserad underrättelseinhämtning som avser utländska förhållanden kan bedrivas också så att kommunikationen sker från Finland med hjälp av kommunikationstjänsterna i ett datanät.

Ibruktagandet av de nya metoder för inhämtande av information som föreslås för Försvarsmakten i fråga om personbaserad underrättelseinhämtning förpliktar militärunderrättelsemyndigheten att försäkra sig om att den personal som utför underrättelseinhämtningen har ändamålsenlig utbildning och att personalen också i övrigt är tillräckligt förtrogen med sina uppgifter. När praktisk utbildning om befogenheterna ges är det delvis möjligt att utnyttja yrkesfärdigheterna hos de tjänstemän som i nuläget tjänstgör i uppgifter som gäller Försvarsmaktens

brottsbekämpning. Dessa tjänstemän har långvarig erfarenhet av sådana uppgifter inom militärt kontraspionage och personbaserad underrättelseinhämtning som avser utredning av brott. Vissa delar av utbildningen kan eventuellt också planeras och genomföras i samarbete med skyddspolisen och genom utbildning som fås genom internationellt samarbete samt genom annan orientering.

Försvarsmakten svarar för reservistutbildningen som en del av det normala systemet med repetitionsövningar för värnpliktiga i enlighet med 32 § i värnpliktslagen. På grund av särdragen i verksamheten är det inte möjligt att skaffa utbildning om befogenheterna genom de åtgärder som avses i lagen om frivilligt försvar (556/2007).

I kapitlet föreskrivs det också om andra metoder för underrättelseinhämtning än sådana metoder som anses vara traditionella. Dessa metoder är radiosignalspaning och underrättelseinhämtning som avser utländska datasystem samt underrättelseinhämtning som avser datatrafik. Metoderna inbegriper informationsinhämtning som utförs uttryckligen med tekniska metoder och där objektet i huvudsak inte är verksamhet mellan personer och information inte kan inhämtas genom att personligen delta i situationen. Dessutom används dessa metoder för underrättelseinhämtning från Finlands territorium när föremålet för underrättelseinhämtning befinner sig utanför Finlands territorium.

I fråga om utövandet av de befogenheter till informationsinhämtning som anges i kapitlet ska man beakta vilket föremål för militär underrättelseinhämtning som det inhämtas information om med metoderna. Enligt det förslag till ändring av 10 § 3 mom. i grundlagen som är under arbete kan hemligheten i fråga om förtroliga meddelanden begränsas genom lag om föremålet är militär verksamhet eller verksamhet som allvarligt hotar den nationella säkerheten.

**20 §.** *Observation och systematisk observation.* I 1 mom. definieras begreppet observation. Observation är möjlig om de allmänna förutsättningar som avses i 10 § uppfylls. Dessutom ska de allmänna principerna beaktas i verksamheten. Observation kan gälla en person eller grupp av personer. Karakteristiskt för åtgärden är att observationer görs obemärkt. Observation kan utföras så att föremålet för informationsinhämtning inte märker att det är föremål för observation, trots att observationen i sig genomförs helt öppet. Det kan sålunda dels vara fråga om att göra iakttagelser i hemlighet och dels om att göra iakttagelser så att syftet med inhämtandet av information hemlighålls.

Momentet avviker från den gällande lagstiftningen om hemligt inhämtande av information på så sätt att i den nämns utöver en grupp av personer också särskilt föremål, ämnen, egendom, utrymmen eller områden. Detta är motiverat med tanke på koherensen i bestämmelserna om metoder för underrättelseinhämtning. I den gällande lagstiftningen nämns de objekt som avses ovan särskilt i bl.a. bestämmelserna om teknisk observation.

Inom underrättelseverksamheten kan det dessutom bedömas vilken betydelse den verksamhet som är föremål för underrättelseinhämtning har för tryggandet av försvaret och den nationella säkerheten när det gäller en viss aktörs resurser och strategiska avsikter att skada Finlands försvar eller nationella säkerhet. När den aktör som är föremål för underrättelseinhämtning har resurser som minst motsvarar de strategiska avsikterna kan man redan tala om en aktör som utgör ett faktiskt hot. Med tanke på i synnerhet vissa resurser kan det vara viktigt att dessa resurser och förflyttningarna av dem kan observeras. På så sätt kan man också indirekt observera hur en viss person rör sig.

Att göra iakttagelser innebär att observatören befinner sig i t.ex. samma utrymme eller situation som den som är föremål för observation samt att det inte sker någon växelverkan mellan observatören och den observerade. Detta utgör inget hinder för växelverkan med den observerade i en situation där det finns risk för att t.ex. inhämtandet av information avslöjas. Observatören kan vid behov dra sig ur en situation med hjälp av växelverkan, i praktiken genom att t.ex. samtala med den observerade.

Föremål för observation kan utöver personer också vara t.ex. en stor mängd av ett visst ämne eller annan egendom som kan användas t.ex. för att orsaka skada som kan jämföras med militär verksamhet. Dessutom är kartläggning och målidentifiering av områden och objekt som är kritiska med tanke på samhällets funktion centrala föremål för militär underrättelseverksamhet som riktar sig mot Finland. Observation kan användas t.ex. för kartläggning av de personer som är intresserade av de objekt som beskrivs ovan.

Vid observation får som stöd för egna sinnesiakttagelser användas bl.a. en kikare, kamera, videokamera, bildförstärkare eller någon annan motsvarande teknisk anordning. Med detta avses i samband med observation upptagning av bilder eller ljud, insamlande av information och behandling av den med bl.a. tekniska anordningar, metoder eller programvaror. Upptagning av bilder och ljud i samband med observation är nödvändigt t.ex. för att dokumentera olika händelser samt för att verifiera dem i efterhand. Den som utför observationen ska under hela den tid som iakttagelser görs inneha hjälpmedel.

Vid observation får enligt 1 mom. de anordningar som avses ovan trots 24 kap. 6 § i strafflagen användas för att göra eller uppta visuella iakttagelser. Bestämmelsen förtydligar gränsdragningen i förhållande till kriminaliseringen av olovlig observation enligt 24 kap. 6 § i strafflagen.

Enligt 2 mom. i den föreslagna paragrafen avses med systematisk observation annan än kortvarig observation av en person eller grupp av personer som med fog kan antas ha samband med ett underrättelseuppdrag. I enlighet med förutsättningarna för användning av metoder för underrättelseinhämtning kan en metod för underrättelseinhämtning användas i hemlighet för den som metoden riktar sig mot, vilket betyder att också vid systematisk observation ska växelverkan med den observerade undvikas.

Med begreppet ”som med fog kan antas ha samband med” avses direkta observationer av den verksamhet som bedrivs av en person eller grupp av personer samt tips från utomstående personer, t.ex. en informationskälla eller internationell samarbetspart, och annan indirekt utredning. Också en utomstående observatör ska utifrån en utredning med fog kunna anta att en person eller grupp av personer har samband med ett underrättelseuppdrag och att information kan inhämtas om personen eller gruppen av personer med avseende på underrättelseuppdraget. Momentet motsvarar bestämmelserna i 5 kap. i den gällande polislagen med den skillnaden att det i bestämmelsen om befogenheter har tagits in ett antagande om begränsning av föremålet för underrättelseinhämtning. Syftet är att förtydliga systematiken i bestämmelsen.

För systematisk observation kan det inte fastställas någon kortaste varaktighet. Den minimitid som behövs för sådan observation är beroende av omständigheterna i det enskilda fallet. Observation kan anses vara systematisk också då observationen inte pågår en längre tid, men upprepas efter en viss tid. När det gäller bedömningen av kortvarigheten har tiden mellan den första och den sista observationsåtgärden betydelse. Typiskt för systematisk observation är att iaktta vad den som är föremål för informationsinhämtning gör och vilka personer han eller hon träffar. Enligt momentet kan endast en i momentet avsedd person eller grupp av personer vara

föremål för systematisk observation. Observation av andra personer än den personen eller gruppen av personer är således möjlig endast som en kortvarig enskild åtgärd, närmast av den anledningen att man för att förvissa sig om att observationsobjektet är det rätta i praktiken måste göra iakttagelser också av andra personer.

Enligt 3 mom. får militärunderrättelsemyndigheterna använda systematisk observation, om detta kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

Kravet på synnerlig vikt uppfylls enligt regeringens proposition med förslag till polislag (HE 224/2010 rd, s. 40–45 samt 94 och 95) när utförande av hemligt inhämtande av information på ett annat sätt annars skulle vara mycket arbetskrävande eller en fördröjning av underrättelseuppdraget skulle medföra särskild fara eller vara oskäligt dyrt. Kravet på synnerlig vikt förutsätter alltså att utförande av ett underrättelseuppdrag på ett annat sätt leder till att fördröjningen av underrättelseuppdraget medför särskild fara för Finland och det finska samhället i och med att den verksamhet som är föremål för militär underrättelseinhämtning kan utvecklas så att den utgör en konkret fara. I fråga om underrättelseverksamhet är det dessutom viktigt att verksamheten inte avslöjas för utomstående, vilket i värsta fall kan äventyra också Finlands försvar och den nationella säkerheten.

Genom systematisk observation får det inte inhämtas information om t.ex. slumpvisa personer, utan inriktningen av observationen mot ett visst objekt ska alltid kunna motiveras. Detta betyder att militärunderrättelsemyndigheten redan på förhand ska ha en aning om att det lönar sig att observera ett visst objekt som är viktigt med avseende på ett underrättelseuppdrag. Underrättelseuppdraget begränsar redan i sig självt de objekt som kan antas kunna ge viktig information. Den som fattar beslut om utövande av befogenheten ska vara övertygad om att man genom att observera just detta objekt kan få information som behövs för ett underrättelseuppdrag.

Inriktningen av befogenheterna enligt paragrafen begränsas av förbudet i 4 mom. mot att rikta utövandet av en befogenhet mot utrymmen som används för stadigvarande boende. Den grundlagstryggade hemfriden omfattar i princip alla 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, GrUU 8/2006 rd s. 2). Den sfär som skyddas av hemfriden definieras dock inte på samma sätt i grundlagen som i t.ex. strafflagen. Av denna orsak får användningen av en metod för underrättelseinhämtning inte riktas mot enligt 24 kap. 11 § i grundlagen hemfridsskyddade bostäder eller övriga utrymmen som är avsedda för boende, om det inte kan visas att platsen faktiskt används för annat boende än boende av permanent natur (GrUU 36/1998 rd, HD 2009:54).

I momentet fastställs också en begränsning som innebär att en teknisk anordning som används vid observation inte får användas vid informationsinhämtning som riktar sig mot en hemfridsskyddad plats. Momentet motsvarar bestämmelsen i 5 kap. 13 § 4 mom. i polislagen.

**21 §**. *Beslut om systematisk observation.* Enligt 1 mom. ska beslut om systematisk observation fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Det är behövligt att föreskriva om beslutsfattande om systematisk observation separat från observation eftersom verksamheten är långvarigare och mer systematisk. Till följd av detta ingriper befogenheten i större utsträckning i skyddet för privatlivet än observation.

Beslut om systematisk observation ska fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

För att nämnda tjänsteman ska ha självständig beslutanderätt i ett ärende ska tjänstemannen vara särskilt förtrogen med eller ha fått särskild utbildning i användningen av metoder för underrättelseinhämtning. Försvarsmakten har ansvar för att ordna utbildningen. Till exempel de tjänstemän som sköter Försvarsmaktens brottsbekämpning har deltagit i så kallade STEK-POV-utbildningar som ordnas inom polisförvaltningen. Utbildning kan ordnas i samarbete med skyddspolisen eller skaffas av internationella samarbetsparter. Försvarsmakten har redan i nuläget långvarig erfarenhet av användning av och utbildning om vissa av de föreslagna metoderna för underrättelseinhämtning, medan skyddspolisen har långvarig erfarenhet av användning av hemliga metoder för inhämtande av information och av hemliga tvångsmedel som genomförs på allmän plats och används av andra än Försvarsmakten. Dessutom ska Försvarsmakten också internt ordna tillräcklig utbildning för tjänstemännen vid militärunderrättelsemyndigheterna och se till att tjänstemännen har tillräcklig utbildning.

Kravet på att beslutsfattaren ska vara förtrogen med utövandet av befogenheter skiljer sig från vad som annanstans i lagstiftningen, såsom i 5 kap. i polislagen, föreskrivs om krav på utbildning. Till följd av grunderna för användningen av metoder för underrättelseinhämtning och de ibland mångtydiga gränsdragningarna mellan metoderna för underrättelseinhämtning är det behövligt att det krävs att en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning förtrogen militärjurist eller annan tjänsteman har tillräckliga kunskaper i användning av metoder för underrättelseinhämtning. Kravet på förtrogenhet uppfylls antingen genom utbildning om hemligt inhämtande av information eller genom tillräcklig erfarenhet av användning av hemligt inhämtande av information.

Kravet på förtrogenhet kan uppfyllas antingen genom utbildning om hemligt inhämtande av information eller genom tillräcklig erfarenhet av användning av hemligt inhämtande av information eller av användning av metoder för underrättelseinhämtning. Dessutom ska en tjänsteman vara förtrogen med lagstiftningen om befogenheter till underrättelseinhämtning. Det finns inget specifikt utbildningsprogram för användning av metoder för underrättelseinhämtning, vilket innebär att tillräcklig förtrogenhet kan erhållas på andra sätt. Militärunderrättelsemyndigheten ska internt pröva vem som anses vara tillräckligt förtrogen med användningen av metoder för underrättelseinhämtning.

Det är ändamålsenligt att i momentet också särskilt nämna en militärjurist. En militärjurist är till följd av sin utbildning förtrogen med i synnerhet lagstiftningsfrågor. Av denna orsak har en militärjurist behövligt kunnande om det utarbetande av motiveringar, den juridiska argumentation och den gränsdragning i mångtydiga situationer som beslutsfattandet förutsätter. Förtrogenhet med användningen av metoder för underrättelseinhämtning kräver tid, vilket innebär att också andra tjänstemän kan fatta beslut när de är tillräckligt förtrogna med en fråga.

I sista hand ansvarar militärunderrättelsemyndighetens chef för bedömningen av att tjänstemännen är tillräckligt förtrogna med uppgifterna. Med uttrycket ”en för uppdraget förordnad” avses att den aktör som inom militärunderrättelsemyndighetens organisation beslutar om placering av personer ska avgöra om en militärjurist eller annan tjänsteman är tillräckligt förtrogna med skötseln av en uppgift. I sista hand ska en organisations chef bedöma uppgiftens lämplighet och graden av förtrogenhet, vilket också betyder att chefen bär ansvar för att en tjänsteman har kompetens att sköta en uppgift.

Enligt 2 mom. får beslut meddelas för högst sex månader åt gången. Beslutsfattarens prövning begränsas av proportionalitetsprincipen, principen om minsta olägenhet, principen om ändamålsbundenhet och principen om icke-diskriminering. Att beslut enligt bestämmelsen får meddelas för högst sex månader innebär dock inte automatiskt att ett beslut alltid får meddelas för sex månader. När man överväger ett besluts giltighetstid ska särskild uppmärksamhet fästas vid proportionalitetsprincipen och principen om minsta olägenhet. Därför ska det både när tillstånd söks och när tillstånd beviljas göras en övervägning från fall till fall av hur länge en metod för underrättelseinhämtning behöver användas.

I 3 mom. i den föreslagna paragrafen föreskrivs det om vad som ska nämnas i yrkandet och beslutet. I momentets 1 punkt avses med det underrättelseuppdrag som ligger till grund för åtgärden ett underrättelseuppdrag enligt 9 § som grundar sig på föremålen för den militära underrättelseinhämtningen enligt 4 § och på en begäran om information enligt 16 § eller på Försvarsmaktens förvaltningsenhets uppdrag. Ett underrättelseuppdrag ska ligga till grund för användningen av en metod för underrättelseinhämtning. Av beslutet ska dessutom framgå syftet med åtgärden, dvs. vad som eftersträvas med användning av en metod för underrättelseinhämtning. Syftet ska fastställas med tillräcklig noggrannhet.

I 2 punkten fastställs att i beslutet ska nämnas vem som är föremål för användningen av en metod för underrättelseinhämtning. En person eller grupp av personer kan vara föremål för systematisk observation. Beslutet ska innehålla ett motiverat antagande om att en viss person eller grupp av personer har samband med ett underrättelseuppdrag.

Vid militär underrättelseinhämtning kan det uppkomma ett behov av att passivt eller aktivt iaktta den verksamhet som bedrivs av en viss grupp av personer. Vid systematisk observation är inhämtandet av information dock snarare passivt. Eftersom det när en metod för underrättelseinhämtning används inte är fråga om verksamhet som syftar till brottsbekämpning, medför identifieringen av en viss person inte att det vid militär underrättelseinhämtning uppkommer ett motsvarande behov av att bedöma de särskilda förutsättningarna för utövande av befogenheter, såsom huruvida det finns anledning att misstänka personen i fråga för ett visst brott eller att anta att personen har gjort sig skyldig till ett brott. Vid militär underrättelseinhämtning är avsikten t.ex. att inhämta information om hur en viss grupp av personer är organiserad, vilka personer som hör till gruppen och hur aktiv gruppen av personer är på vissa områden samt de olika former av verksamhet som gruppen bedriver.

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, såsom att förbereda militär verksamhet som riktar sig mot t.ex. Finland 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 observerbara strukturer, såsom befälshierarkierna 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. En grupp av personer ska kunna identifieras också på andra sätt än enbart på basis av de egenskaper som avses i 8 § i denna proposition. Således räcker det inte med att fastställa en grupp av personer med stöd av t.ex. medborgarskap, utan en grupp av personer ska fastställas med användning av andra kriterier som definierar gruppen, såsom med stöd av de kriterier som nämns ovan.

Informationen kan ha betydelse vid beslutsfattandet om andra metoder för underrättelseinhämtning på såväl operativ som strategisk nivå. Vid systematisk observation som utförs i samband med militär underrättelseinhämtning har det när befogenheten utövas betydelse om objektet med fog kan antas ha samband med ett underrättelseuppdrag. En förutsättning för utövandet av befogenheten är att systematisk observation ska ha synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

I enlighet med principen om minsta olägenhet ska utövandet av befogenheten i första hand riktas mot en viss person. I samband med underrättelseverksamhet kan det dock vara behövligt att reda ut vilka som hör till en viss grupp av personer eller om det inom en viss grupp finns t.ex. en militär gruppering samt att granska den verksamhet som personer från en främmande underrättelsetjänst bedriver på ett visst område. I det fallet att informationsinhämtning riktar sig mot en viss grupp av personer och informationsinhämtningen inte preciseras till en enskild person eller enskilda personer som befinner sig i Finland behöver den underrättelse som avses i 86 § inte göras. Om användningen av en metod för underrättelseinhämtning riktar sig mot en viss grupp av personer som befinner sig i Finland och en person ur gruppen identifieras så att hans eller hennes identitet klarnar ska 86 § som gäller underrättelse om användning av en metod för underrättelseinhämtning tillämpas på underrättelsen på samma sätt som när systematisk observation riktar sig mot en person.

Liksom i fråga om de övriga metoderna för underrättelseinhämtning ska också ett beslut om systematisk observation innehålla en redogörelse för de fakta som inriktningen av den systematiska observationen av en person eller grupp av personer grundar sig på så att den som fattar beslut om användningen av en metod har möjlighet att noga pröva beslutet. När beslut om användningen av en metod för underrättelseinhämtning fattas av en underrättelsemyndighet är omständigheter som är viktiga med tanke på beslutet av särskild betydelse för att möjliggöra både intern övervakning och den rättsliga övervakning som utförs av underrättelseombudsmannen.

Momentets 3 punkt är av betydelse med tanke på beslutsfattandet. Enligt punkten ska i yrkandet och beslutet nämnas de fakta som förutsättningarna för och inriktningen av den systematiska observationen grundar sig på. Att fakta ska läggas fram för beslutsfattaren förpliktar underrättelsemyndigheten att lägga fram och motivera fakta på basis av vilka beslutsfattaren kan dra sina egna slutsatser om huruvida förutsättningarna uppfylls. Dessa förutsättningar är de allmänna förutsättningar för användning av metoder för underrättelseinhämtning som avses i 11 § och de förutsättningar som nämns i 20 §, som gäller befogenhet. I beslutet ska vidare läggas fram tillräckliga fakta om underrättelseuppdraget och det i 4 § avsedda föremål för militär underrättelseinhämtning som ligger till grund för uppdraget samt om den begäran om information som avses i 13 § eller något annat uppdrag. Med tanke på proportionalitetsprincipen är det särskilt viktigt hur allvarlig verksamheten i fråga är.

Enligt 4 punkten i momentet ska i beslutet nämnas giltighetstiden för beslutet om systematisk observation.

I beslutet ska enligt 5 punkten i momentet nämnas den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar den systematiska observationen. Den ledande och övervakande tjänstemannen är mycket viktig vid övervakningen av användningen av metoder för underrättelseinhämtning. Det är fråga om normal chefsövervakning. Den ledande och övervakande tjänstemannen ska ingripa i eventuella oegentligheter och allmänt styra verksamheten under den tid som en metod för underrättelseinhämtning används. Den tjänsteman som svarar för styrningen och övervakningen kan också

granska de handlingar och upptagningar som producerats under den tid som en metod för underrättelseinhämtning använts.

Enligt 6 punkten ska i yrkandet eller beslutet nämnas eventuella begränsningar och villkor för den systematiska observationen. I beslutet kan det fastställas begränsningar och användarvillkor för den systematiska observationen.

**22 §.** *Förtäckt inhämtande av information.* Enligt 1 mom. avses med *förtäckt inhämtande av information* inhämtande av information genom kortvarig interaktion med en viss person där falska, vilseledande eller förtäckta uppgifter används för att hemlighålla militärunderrättelsemyndigheternas uppdrag.

Som en situation där förtäckt inhämtande av information används kan nämnas t.ex. en situation där en tjänsteman i en vardaglig situation måste fråga ett objekt som har samband med ett underrättelseuppdrag om objektets resmål eller reda ut objektets språkkunskaper på ett sådant sätt att tjänstemannen inte behöver avslöja sin egen identitet.

Dessutom kan befogenheten innebära t.ex. att en försändelse till en viss person levereras av en person som utger sig för att vara ett bud. I sådana situationer är det möjligt att försändelsen tas emot av någon annan person än den som avses i 1 mom. Det kan också vara fråga om förtäckt inhämtande av information då en militärunderrättelsemyndighets tjänsteman utger sig för att vara en servitör i en restaurang för att kunna inhämta information i närheten av en viss person. Någon exakt tidsgräns kan inte anges för hur länge förtäckt inhämtande av information får pågå, eftersom den andra parten genom sina åtgärder kan göra att situationen drar ut på tiden, trots att syftet med inhämtandet av information redan har uppnåtts. Om man drar sig ur en situation på ett onaturligt sätt kan detta avslöja att information inhämtats.

Förtäckt inhämtande av information kan också utföras i datanät. Även i detta fall ska särskild uppmärksamhet fästas vid gränsdragningen mellan förtäckt inhämtande av information och en täckoperation. Vid förtäckt inhämtande av information som sker i datanät ska det också i fortsättningen vara fråga om kortvarig interaktion och därmed anslutet inhämtande av information. Detta kan bli aktuellt t.ex. i samband med registrering för ett visst diskussionsforum och uppföljning av den debatt som förs utan att direkt ta kontakt med en viss debattör.

Till åtskillnad från observation och systematisk observation faller det sig naturligt att utöva befogenheten uttryckligen för att personligen träffa ett objekt eller inleda någon motsvarande interaktion med ett objekt som har samband med ett underrättelseuppdrag, dock inte den form av längre umgänge och sådana särskilda förtroendeförhållanden som när det är fråga om en täckoperation. Vid förtäckt inhämtande av information är det således inte aktuellt med infiltration.

Befogenheten får inte utövas i syfte att kringgå bestämmelserna som gäller täckoperationer. Avsikten är inte heller i övrigt att ersätta bestämmelserna om täckoperationer. Att inleda en täckoperation är dock onödigt invecklat med tanke på en kortvarig enskild situation av denna typ där information inhämtas. Kravet på att en militärunderrättelsemyndighets tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning ska ha utbildning medför att det är mycket viktigt att en sådan tjänsteman är medveten om gränsen mellan inhämtande av information och en täckoperation för att befogenheten inte ska utövas så att det i själva verket är fråga om en täckoperation. Med hjälp av utbildning kan man även minska risken för att inhämtandet av information avslöjas samt främja verksamhetens resultat. Dessa

aspekter har ännu starkare än förtäckt inhämtande av information samband med täckoperationer och bevisprovokation genom köp.

Utmärkande för verksamheten är dessutom att endast falska, vilseledande eller förtäckta uppgifter används. Som ett exempel kan nämnas användning av ett transportbolags overall och namnskylt. En sådan skyddsmetod kan användas endast för att hemlighålla Försvarsmaktens underrättelsetjänsts uppdrag, med andra ord för att förhindra att inhämtandet av information avslöjas. Användningen av en metod för underrättelseinhämtning kan skyddas i enlighet med 72 §.

I 2 mom. i den föreslagna paragrafen föreskrivs det om förutsättningarna för användning av förtäckt inhämtande av information. En förutsättning för användning är en sådan allmän förutsättning för användning av metoder för underrättelseinhämtning som det redogörs för i detaljmotiveringen till 11 §.

Enligt 3 mom. i den föreslagna paragrafen är förtäckt inhämtande av information inte tillåtet i en bostad ens med bostadsinnehavarens medverkan. Denna lösning motsvarar grundlagsutskottets ståndpunkt i riksdagsbehandlingen av den nya tvångsmedelslagen (GrUU 66/2010 rd).

**23 §.** *Beslut om förtäckt inhämtande av information.* Enligt 1 mom. ska beslut om förtäckt inhämtande av information fattas av Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. På samma sätt som det konstateras i detaljmotiveringen till 20 § är en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman skyldig att identifiera om det i en viss situation är fråga om användning av förtäckt inhämtande av information eller en täckoperation.

I och med kravet på att en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman ska ha utbildning har den aktör som fattar beslut särskild kännedom om gränsen mellan förtäckt inhämtande av information och en täckoperation, vilket ska bidra till att befogenheten inte utövas så att det i själva verket är fråga om en täckoperation. Risken för att avslöjas kan minskas också genom utbildning.

Enligt 2 mom. ska beslutet om förtäckt inhämtande av information fattas skriftligen. I beslutet ska följande nämnas: 1) åtgärden och dess syfte samt det underrättelseuppdrag som ligger till grund för åtgärden, 2) den person eller grupp av personer som är föremål för åtgärden, 3) de fakta som förutsättningarna för och inriktningen av det förtäckta inhämtandet av information grundar sig på, 4) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar det förtäckta inhämtandet av information, 5) den planerade tidpunkten för genomförandet av åtgärden, 6) eventuella begränsningar och villkor för det förtäckta inhämtandet av information.

Liksom i fråga om de övriga metoderna för underrättelseinhämtning ska också i beslutet om förtäckt inhämtande av information nämnas de fakta som inhämtandet av information om personer eller grupper av personer grundar sig på och på basis av vilka en utomstående observatör kan dra sina egna slutsatser om huruvida förutsättningarna för användning av en metod för underrättelseinhämtning uppfylls.

Med en åtgärd avses en faktisk åtgärd för förtäckt inhämtande av information, såsom att utge sig för att vara en servitör eller ett bud. En särskild förutsättning för utövandet av befogenhet-

en är att det vid Försvarsmaktens underrättelsetjänst utses en ansvarig tjänsteman som har i uppgift att bl.a. se till att verksamheten de facto inte utgör en täckoperation och att den som utger sig för att vara en taxichaufför inte börjar skapa ett förtroligt förhållande med sin kund.

När det gäller förtäckt inhämtande av information förutsätts det inte att tidpunkten då verksamheten inleds och avslutas anges med exakt klockslag eftersom det vanligen är fråga om att en enskild åtgärd utförs på en tidpunkt som inte anges på förhand. Det är möjligt att förtäckt inhämtande av information sker en viss dag eller en viss vecka.

Beslutsfattaren kan i fråga om förtäckt inhämtande av information fastställa begränsningar och uppställa villkor på samma sätt som vid användningen av andra metoder för underrättelseinhämtning. Begränsningarna kan bero t.ex. på proportionalitetsprincipen samt på ändamålsenlighets-, rättssäkerhets- och arbetarskyddsaspekter.

Beslutsfattaren kan i fråga om förtäckt inhämtande av information fastställa begränsningar och uppställa villkor på samma sätt som vid användningen av andra metoder för underrättelseinhämtning. Begränsningarna kan bero t.ex. på proportionalitetsprincipen samt på ändamålsenlighets-, rättssäkerhets- och arbetarskyddsaspekter.

Enligt 3 mom. ska beslutet vid behov ses över när omständigheterna förändras. I samband med en underrättelseoperation är det möjligt att föremålet för informationsinhämtning preciseras, vilket innebär att användningen av en metod för underrättelseinhämtning ska riktas mot den person eller grupp av personer som man ursprungligen avsåg att inhämta information om. Detta förpliktar den som ansvarar för en åtgärd att kontrollera att förutsättningarna för förtäckt inhämtande av information uppfylls och att följa upp behovet av inhämtande av information, i synnerhet då skillnaden i tid mellan beslutet och genomförandet av åtgärden är betydande.

I 4 mom. fastställs det att om åtgärden inte tål uppskov, behöver ett beslut om förtäckt inhämtande av information inte upprättas i skriftlig form före åtgärden vidtas. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter det att åtgärden har vidtagits.

Bestämmelsen är ny i förhållande till den gällande lagstiftningen om hemliga metoder för inhämtande av information. Militärunderrättelsemyndigheten kan om situationen kräver det utan dröjsmål börja genomföra förtäckt inhämtande av information. Detta innebär inte att kravet på att beslutet ska upprättas i skriftlig form frångås utan möjliggör att en metod för underrättelseinhämtning kan användas i en brådskande situation. Beslutet om förtäckt inhämtande av information ska upprättas i skriftlig form genast när det är möjligt. I brådskande situationer ska det med tanke på arbetssäkerheten och rättsskyddet för den som vidtar en åtgärd ses till att denna muntligen har getts information om de uppgifter som ska nämnas i beslutet. I brådskande situationer accentueras den beslutsfattande tjänstemannens yrkesskicklighet och kunnande.

**24 §.** *Teknisk avlyssning*. Enligt 1 mom. har militärunderrättelsemyndigheten rätt att för att utföra ett underrättelseuppdrag inhämta information med stöd av teknisk avlyssning av ett samtal eller meddelande som inte är avsett för utomstående. Teknisk avlyssning skiljer sig från observation i det avseendet att man vid teknisk avlyssning använder utplacerade tekniska anordningar, metoder eller programvaror.

Med teknisk avlyssning avses att en viss persons samtal eller meddelande som inte är avsett för utomstående och i vilket avlyssnaren inte deltar, trots 24 kap. 5 § i strafflagen avlyssnas, upptas eller behandlas på något annat sätt med hjälp av en teknisk anordning, metod eller pro-

gramvara i syfte att ta reda på innehållet i samtalet eller meddelandet eller utreda deltagarnas verksamhet. I momentet nämns utöver avlyssning och upptagning också annan behandling av ett samtal eller meddelande samt teknikneutralt utöver tekniska anordningar också metoder och programvaror.

Teknisk avlyssning utgör ofta ett komplement till systematisk observation. Med teknisk avlyssning kan man få information om t.ex. när en person som är föremål för systematisk observation sätter sig i rörelse, varefter man på nytt aktivt kan inleda systematisk observation. Syftet med teknisk avlyssning är att inhämta endast information som har samband med ett underrättelseuppdrag. Det är dock sannolikt att också andra personer än personer som är relevanta med avseende på ett underrättelseuppdrag oundvikligen blir föremål för avlyssning på grund av att förutsättningarna för inriktning av denna metod för underrättelseinhämtning (person, grupp av personer, utrymme eller annan plats) är mer omfattande än befogenheterna till brottsbekämpning. Av denna orsak är det nödvändigt att bl.a. information som inte har samband med ett underrättelseuppdrag förstörs omedelbart, om man märker att informationen inte får användas med stöd av paragrafen om användning av en uppgift som inte anknyter till ett underrättelseuppdrag. Med tanke på militär underrättelseinhämtning kan dock teknisk avlyssning som riktar sig mot ett utrymme vara viktig också för att reda ut att ett visst utrymme inte används.

Teknisk avlyssning täcker också situationer där man tekniskt observerar tangentbordet till en dataterminal i samband med sändandet av e-post.

Teknisk avlyssning är möjlig om inhämtandet av information ska riktas mot en person som berövats sin frihet. Trots att militär underrättelseinhämtning inte ger behörighet att gripa en person kan underrättelseinhämtning bli aktuell i fråga om personer som gripits av andra myndigheter, såsom personer som gripits av Tullen eller gränsbevakningsväsendet.

Teknisk avlyssning får inte riktas mot ett utrymme som används för stadigvarande boende. Det saknar betydelse var en teknisk anordning, metod eller programvara installeras. Av betydelse är på vad teknisk avlyssning inriktas.

Försvarsmakten har enligt 4 kap. i lagen om militär disciplin och brottsbekämpning inom försvarsmakten rätt att gripa personer när de förutsättningar som anges i den lagen uppfylls. Förutsättningarna har samband med de brott som avses i 2 § i militära rättegångslagen (326/1983). Militärunderrättelsemyndigheterna kan i dessa situationer med tanke på underrättelseinhämtningen behöva inhämta information om en gripen person. Av denna anledning kan teknisk avlyssning riktas också mot en gripen person genom beslut av domstol.

I definitionen av teknisk avlyssning fastställs förhållandet mellan en metod för inhämtande av information och verksamhet som är förbjuden enligt strafflagen. I 24 kap. 5 § 1 mom. i strafflagen kriminaliseras olovlig avlyssning. Med uttrycket ”trots 24 kap. 5 § i strafflagen” avses att man i samband med teknisk observation inte gör sig skyldig till olovlig avlyssning eller olovlig observation, förutsatt att metoden för underrättelseinhämtning används på rätt sätt. Detta innebär att beslutet om användning av teknisk avlyssning har tillkommit i rätt ordning och att den tekniska avlyssningen används lagenligt.

Teknisk avlyssning kan utföras i realtid eller passivt. Vid teknisk avlyssning som utförs i realtid ska man fästa uppmärksamhet vid om den person som är föremål för användning av en metod för underrättelseinhämtning befinner sig i ett utrymme eller inte samt avbryta den tekniska avlyssningen för den tid som den person som är föremål för användningen av en metod för

underrättelseinhämtning avlägsnar sig från utrymmet för en längre tid än endast ett ögonblick. Vid passiv teknisk avlyssning utförs det som nämns ovan med stöd av de skyldigheter som fastställts för militärunderrättelsemyndigheterna i fråga om granskning av upptagningar samt förstöring av irrelevanta och onödiga uppgifter.

Definitionen av begreppet teknisk avlyssning sammanhänger med det faktum att inhämtande av information om t.ex. ett högljutt samtal i ett offentligt utrymme inte förutsätter användning av metoder för underrättelseinhämtning. Detsamma gäller ett samtal som avlyssnaren deltar i. Det är inte heller fråga om teknisk avlyssning då man med en avlyssningsanordning ger akt på de ljud som orsakas av en misstänkt persons rörelser. Däremot är det fråga om teknisk avlyssning då man med en teknisk anordning avlyssnar eller upptar vad den andra parten säger under ett telefonsamtal, dvs. då avlyssningen riktas mot de ljudvågor som samtalet alstrar.

Att med en teknisk anordning avlyssna en viss person betraktas inte som teknisk avlyssning, om anordningen inte är utplacerad på platsen. I dessa fall är det, beroende på åtgärdens varaktighet, fråga om observation eller systematisk observation. Kravet på att en anordning ska ha utplacerats på en viss plats innebär i praktiken att teknisk observation inte är en kortvarig åtgärd. Med begreppet ”utplacerad” avses t.ex. att en anordning, metod eller programvara har fästs i en vägg eller ett tak eller på något annat lämpligt ställe. Kännetecknande för teknisk avlyssning är dessutom, på grund av definitionen, att anordningen, metoden eller programvaran i allmänhet följer objektet utan att militärunderrättelsemyndigheten samtidigt behöver göra iakttagelser och vara närvarande. Det föreskrivs nedan om installation och avinstallation av spårningsanordningar. Om det är fråga om sådan spårning av en person som innebär att en tjänsteman i realtid använder en anordning som tjänstemannen innehar för att göra iakttagelser om personen, betraktas åtgärden som systematisk observation.

I 1 mom. nämns utöver avlyssning och upptagning också annan behandling av ett samtal eller meddelande. Med detta avses bl.a. teknisk observation av användningen av tangentbordet till en dataterminal i samband med sändandet av e-post, vilket också kallas för tangentbordsavlyssning. I definitionsbestämmelsen i momentet konstateras det uttryckligen att syftet med teknisk avlyssning också är att ta reda på innehållet i ett samtal eller meddelande. Syftet kan utöver att ta reda på det egentliga innehållet även vara att identifiera parterna i ett samtal eller en kommunikation eller att i något annat avseende ta reda på vad en misstänkt person sysslar med.

I detta sammanhang är det emellertid skäl att understryka betydelsen av de principer som ska tillämpas vid militär underrättelseinhämtning då den tekniska avlyssningen utförs på ett sätt som i avsaknad av befogenhet skulle innebära att observatören gör sig skyldig till olovlig avlyssning eller olovlig observation.

I 2 mom. föreskrivs det om vem och vad teknisk avlyssning kan riktas mot samt under vilka förutsättningar teknisk avlyssning får användas. Teknisk avlyssning får inriktas på en person eller grupp av personer, om detta kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag. Förutsättningen synnerlig vikt beskrivs i detaljmotiveringen till 20 §.

Teknisk avlyssning kan t.ex. utföras så att den de facto riktas mot ett sådant utrymme eller en sådan plats som får avlyssnas. Det är då fråga om s.k. utrymmesavlyssning. I de situationer som avses i momentet kan teknisk avlyssning inte genomföras som en kontinuerlig spårningsåtgärd t.ex. på grund av risken för att avslöjas, utan endast i vissa utrymmen och på vissa platser som har betydelse för ett underrättelseuppdrag. Som ett exempel kan nämnas en situation

där en misstänkt person som är viktig med avseende på underrättelseinhämtningen förflyttar sig från en allmän plats till ett lagerutrymme. Den tjänsteman som utför underrättelseinhämtningen kan inte utan att avslöja sig följa personen till utrymmet i fråga, utan den tekniska avlyssningen måste utföras på något annat sätt. Detta innebär i praktiken att utrymmet i fråga på förhand måste förses med avlyssningsanordningar. Med teknisk avlyssning kan man dock också få information om att ett visst utrymme eller en annan plats inte används för den verksamhet som är föremål för underrättelseuppdraget.

Teknisk avlyssning kan riktas mot en person eller grupp av personer som befinner sig i ett sådant hemfridsskyddat utrymme som avses i 24 kap. 11 § i strafflagen, förutsatt att utrymmet inte används för stadigvarande boende. Det har ingen betydelse var en teknisk anordning, metod eller programvara installeras när teknisk avlyssning riktar sig mot verksamhet som inte bedrivs i ett utrymme som används för stadigvarande boende.

Vid användning av teknisk avlyssning ska avgränsningen av utrymmen som används för stadigvarande boende fastställas från fall till fall. Det saknar dock betydelse var en teknisk anordning, metod eller programvara installeras. Av betydelse är på vad teknisk avlyssning inriktas.

**25 §.** *Beslut om teknisk avlyssning.* Enligt 1 mom. ska beslut om teknisk avlyssning av en person som har berövats sin frihet fattas av domstol. Om ärendet inte tål uppskov, får beslut om teknisk avlyssning fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman till dess 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.

Med en person som har berövats sin frihet avses en häktad eller anhållen person eller en person som har gripits på någon annan lagenlig grund och berövats sin frihet. I fråga om avlyssning förutsätts det inte att den person som är föremål för avlyssning måste befinna sig i en cell eller avtjäna sitt straff i en straffanstalt eller vara isolerad i en tvångsinrättning, vara häktad eller befinna sig i polisens förvaringslokaler. Det är onödigt att nämna denna förutsättning eftersom en person som har berövats sin frihet i praktiken kan avlyssnas endast i de utrymmen som han eller hon får besöka eller vistas i.

Möjliggörande av beslut i brådskande situationer motiveras av den operativa verksamhetens art. Det kan snabbt uppkomma en situation där man inte hinner ansöka om tillstånd av domstolen utan att förlora viktig information om ett objekt som har samband med ett underrättelseuppdrag. Det kan med tanke på situationen vara behövligt att få information om vad personer samtalar om. I detta fall kan en tjänsteman som utför militär underrättelseinhämtning t.ex. med sin smarttelefon spela in ett samtal utan att själv delta i det.

Enligt 2 mom. ska beslut om annan teknisk avlyssning än den som avses i 1 mom. fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Beslutsfattaren finns och beslutsfattandet görs på samma nivå som vid systematisk observation enligt 20 §. I beslutet ska på motsvarande sätt varje person eller grupp av personer som har samband med underrättelseuppdraget nämnas med tillräcklig noggrannhet.

I vissa situationer kan man med teknisk avlyssning inhämta information också om kommunikation som åtnjuter skydd för förtroliga meddelanden. Kommunikationen ska i praktiken gälla en diskussion mellan två personer. Ingripandet i förtrolig kommunikation utgör dock inte ett

lika allvarligt ingripande i de grundläggande fri- och rättigheterna som teleavlyssning, vilket innebär att beslut kan fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman.

Enligt 3 mom. får beslut om teknisk avlyssning fattas för högst sex månader åt gången. Beslutets giltighetstid är längre än t.ex. den giltighetstid som fastställs för motsvarande befogenheter till brottsbekämpning. Detta är motiverat med tanke på den militära underrättelseinhämtningens uppgifter, grunden för användning av metoder för underrättelseinhämtning och användningsändamålet. Underrättelseinhämtning tar längre tid än brottsbekämpning och underrättelseuppdragen är noga planerade på förhand. Syftet med ett underrättelseuppdrag kan t.ex. vara att samla in information om vad målstatens väpnade styrkor sysslar med och därmed anslutna omständigheter. Om föremålet för ett underrättelseuppdrag är betydande kan det ta också mycket lång tid. Till exempel underrättelseinhämtning som gäller en främmande stats intentioner kan i praktiken vara fortgående. Avsikten med underrättelseinhämtning är inte att förhindra eller reda ut ett enskilt brott utan att samla in information i ett tidigt skede för att få en helhetsbild. Bestämmelsen möjliggör att man med ett enda tillståndsbeslut kan utföra förutseende och mer långvarigt inhämtande av information.

Metoder för underrättelseinhämtning får inte användas för att förhindra, avslöja eller reda ut enskilda brott och den information som fås med metoderna ska i princip inte användas i anslutning till brott. Undantag från denna huvudregel anges dock i 6 kap.

Den tid på sex månader som avses i bestämmelsen innebär dock inte automatiskt att tillstånd alltid ges och beslut alltid fattas för sex månader åt gången. Uttrycket ”för högst sex månader åt gången” förutsätter prövning enligt proportionalitetsprincipen och principen om minsta olägenhet. När beslut fattas ska man därför från fall till fall överväga hur länge en metod för underrättelseinhämtning behöver användas.

Enligt 2 mom. ska beslut om annan teknisk avlyssning än den som avses i 1 mom. fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

I 4 mom. föreskrivs det om vad som ska nämnas i ett yrkande och i ett beslut om teknisk avlyssning.

I momentets 1 punkt avses med det underrättelseuppdrag som ligger till grund för åtgärden ett underrättelseuppdrag enligt 9 § som grundar sig på de föremål för militär underrättelseinhämtning som avses i 4 § och på en begäran om information enligt 16 § eller Försvarsmaktens uppdrag. Ett underrättelseuppdrag ska ligga till grund för användningen av en metod för underrättelseinhämtning. Av yrkandet och beslutet ska dessutom framgå syftet med åtgärden, dvs. vad som eftersträvas med användningen av en metod för underrättelseinhämtning. Syftet ska fastställas med tillräcklig noggrannhet.

I 2 punkten fastställs att i yrkandet och beslutet ska nämnas vem eller vad åtgärden riktas mot. Enligt punkten kan teknisk avlyssning riktas mot en person eller grupp av personer. I beslutet ska det med fog visas att en viss person eller grupp av personer har samband med ett underrättelseuppdrag.

Enligt punkten kan teknisk avlyssning dessutom riktas mot ett utrymme eller en plats av annat slag. Med utrymme avses en plats som avgränsas av väggar och ett tak eller motsvarande konstruktioner. Ett utrymme åtskiljs alltså på vissa konstruktionsmässiga sätt från en plats (allmän

eller privat plats). Med någon annan plats avses en plats utanför ett utrymme som avgränsas av väggar och ett tak eller motsvarande konstruktioner, t.ex. en affärsfastighets gårdsplan.

Syftet med teknisk avlyssning är att inhämta information endast för ett underrättelseuppdrag. Det är dock sannolikt att också andra personer än personer som är relevanta med avseende på militär underrättelseinhämtning oundvikligen blir föremål för avlyssning på grund av att förutsättningarna för inriktning av metoder för underrättelseinhämtning (person, grupp av personer, utrymme eller någon annan plats) är mer omfattande än för brottsbekämpning. Denna obalans rättas till genom bl.a. bestämmelserna om underrättelseskyldighet och om rätt till underrättelse samt den rättsliga övervakning som underrättelseombudsmannen riktar mot militärunderrättelsemyndigheterna. Med avlyssning av utrymmen försöker man i princip få information om de personer som befinner sig i utrymmet och om interaktionen mellan dem, men det kan med avseende på underrättelseuppdraget också ha betydelse att reda ut att ett visst utrymme inte används för den verksamhet som är föremål för underrättelseuppdraget.

När teknisk avlyssning riktar sig mot någon annan plats än ett utrymme ska man i yrkandet och beslutet så exakt som möjligt ange storleken på det område som är föremål för teknisk avlyssning. Det område som är föremål för teknisk avlyssning ska i mån av möjlighet avgränsas så att det är så litet som möjligt.

Vid användningen av teknisk avlyssning ska gränsdragningen mellan utrymmen som används för stadigvarande boende och andra platser fastställas från fall till fall när det övervägs om förutsättningarna för teknisk avlyssning uppfylls. Teknisk avlyssning innebär att den som beslutar om denna metod för underrättelseinhämtning är skyldig att göra en avvägning och vid behov ta reda på hur saker och ting förhåller sig. Om ett utrymme eller någon annan plats klassificeras som ett utrymme som används för stadigvarande boende kan denna metod för underrättelseinhämtning inte användas. Denna premiss kan upphävas om en utredning stöder motsatsen. Till exempel en kontorslokal kan de facto användas för boende (t.ex. HD 2009:54) medan en bostadslägenhet kan användas som kontor.

Momentets 3 punkt har betydelse med tanke på beslutsfattandet. Enligt punkten ska i ett yrkande och i ett beslut nämnas de fakta som förutsättningarna för och inriktningen av den tekniska avlyssningen grundar sig på. Att fakta ska läggas fram för beslutsfattaren förpliktar underrättelsemyndigheten att lägga fram och motivera fakta på basis av vilka beslutsfattaren kan dra sina egna slutsatser om huruvida förutsättningarna uppfylls. De nämnda förutsättningarna gäller de allmänna förutsättningar för användning av metoder för underrättelseinhämtning som avses i 11 § och de förutsättningar som nämns i 24 §, som gäller befogenhet. I yrkandet och beslutet ska vidare läggas fram tillräckliga fakta om underrättelseuppdraget och det i 4 § avsedda föremål för militär underrättelseinhämtning som ligger till grund för uppdraget samt om den i 13 § avsedda begäran om information eller något annat av Försvarsmaktens interna uppdrag. Med tanke på proportionalitetsprincipen är det särskilt viktigt hur allvarlig verksamheten i fråga är.

Enligt momentets 4 punkt ska i ett yrkande och i ett beslut nämnas giltighetstiden för beslutet om teknisk avlyssning med angivande av klockslag.

I ett yrkande och i ett beslut ska enligt 5 punkten nämnas den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar den tekniska avlyssningen.

Enligt 6 punkten ska i ett yrkande och i ett beslut nämnas eventuella begränsningar och villkor för den tekniska avlyssningen. I beslutet kan det fastställas begränsningar och användarvillkor för den tekniska avlyssningen.

**26 §.** *Optisk observation.* I 1 mom. definieras begreppet optisk observation. Med *optisk observation* avses att man trots 24 kap. 6 § i strafflagen iakttar eller gör upptagningar av en viss person eller grupp av personer eller av ett utrymme eller någon annan plats med en kamera eller andra utplacerade tekniska anordningar, metoder eller programvaror.

Liksom teknisk avlyssning har optisk observation också i väsentlig grad samband med systematisk observation. Med optisk observation kan man få information om t.ex. när en person som är föremål för underrättelseinhämtning sätter sig i rörelse, varefter man kan inleda systematisk observation. Dessutom kan optisk observation bli aktuell när man vid en träff med en informationskälla med optisk observation inhämtar information om personer som rör sig i området, såsom det intresse som en annan stats underrättelsetjänst visar för informationskällan. Med optisk observation kan man också genomföra informationsinhämtning som inte är möjlig eller säker med t.ex. systematisk observation utan att militärunderrättelsemyndighetens närvaro avslöjas.

Liksom i definitionen av teknisk avlyssning konstateras det också i definitionen av optisk observation att optisk observation riktas mot en viss person eller grupp av personer. Optisk observation kan dock riktas också mot ett visst utrymme eller någon annan plats. På ett teknikneutralt sätt nämns i bestämmelsen utöver olika kameror också andra tekniska anordningar, metoder och programvaror. Optisk observation skiljer sig från observation och systematisk observation i det avseendet att man vid optisk observation använder utplacerade tekniska anordningar, metoder eller programvaror.

På samma sätt som i definitionen av teknisk avlyssning fastställs också i definitionen av optisk observation denna metods förhållande till verksamhet som är förbjuden enligt strafflagen. Enligt 24 kap. 6 § 1 mom. i strafflagen gör sig den skyldig till olovlig observation som obehörigen med en teknisk anordning 1) iakttar eller avbildar en person som vistas på en hemfridsskyddad plats eller på en toalett, i ett omklädningsrum eller på någon annan motsvarande plats, eller 2) på ett integritetskränkande sätt iakttar eller avbildar en person som vistas i en sådan byggnad eller lokal eller på ett sådant omgärdat gårdsområde som avses i 3 § (brott mot offentlig frid) och dit allmänheten inte äger tillträde. Den hänvisning till strafflagen som finns i momentet innebär att man i samband med observationen inte gör sig skyldig till olovlig observation, förutsatt att metoden för underrättelseinhämtning används på rätt sätt. Detta avser att beslutet om användning av optisk observation har tillkommit i rätt ordning och att observationen används i enlighet med lagen.

När det gäller optisk observation ska principerna för militär underrättelseinhämtning beaktas. Detta gäller i synnerhet de utrymmen och andra platser som avses i 24 kap. 6 § 1 mom. 1 punkten i strafflagen. I enlighet med proportionalitetsprincipen ska vid avvägningen av användningen av en metod för underrättelseinhämtning beaktas i vilken utsträckning användningen leder till kränkningar av rättigheter, i detta fall hemfridsskyddet och integritetsskyddet. Också de allmänna principer som styr den militära underrättelseverksamheten ska beaktas. I synnerhet toaletter, omklädningsrum och andra motsvarande utrymmen får inte vara föremål för optisk observation utan vägande skäl.

Optisk observation kan genomföras också på andra sätt än med hjälp av en myndighets anordningar. Den kan utföras t.ex. så att den kameraövervakningsutrustning som en stad äger riktas

mot en viss misstänkt person som militärunderrättelsemyndigheten är intresserad av. Om däremot endast bildmaterial som eventuellt stöder ett underrättelseuppdrag överlämnas till militärunderrättelsemyndigheten från en stads kameraövervakningssystem och upptagningen av materialet skett utanför militärunderrättelsemyndighetens kontroll och inte ligger i militärunderrättelsemyndighetens intresse, är det inte fråga om optisk observation.

Kravet på att utrustningen ska ha placerats ut på en viss plats innebär i praktiken att optisk observation inte är en kortvarig åtgärd. Med begreppet utplacerad avses t.ex. att en anordning, metod eller programvara har fästs i en vägg eller ett tak eller på något annat lämpligt ställe. Kännetecknande för optisk observation är dessutom, på grund av definitionen, att anordningen, metoden eller programvaran i allmänhet följer objektet utan att militärunderrättelsemyndigheten samtidigt behöver göra iakttagelser och vara närvarande. Det föreskrivs nedan om installation och avinstallation av spårningsanordningar. Om det är fråga om sådan spårning av en person som innebär att en tjänsteman i realtid använder en anordning som han eller hon innehar för att göra iakttagelser om personen ska åtgärden betraktas som observation eller systematisk observation.

Enligt 2 mom. får militärunderrättelsemyndigheternas tjänstemän för att utföra ett underrättelseuppdrag inrikta optisk observation på en person som befinner sig utanför ett utrymme som används för stadigvarande boende. Denna metod för underrättelseinhämtning kan riktas mot utrymmen eller andra platser där det kan antas att den person som är föremål för observationen sannolikt befinner sig eller som de kan antas besöka.

Liksom i fråga om regleringen av teknisk avlyssning framgår det av momentet att föremål för optisk observation är en viss person eller grupp av personer, men observationen kan genomföras så att den riktas mot ett visst utrymme som har en tillräckligt nära koppling med personen eller gruppen av personer i fråga. Till denna del kan det hänvisas till vad som i detaljmotiveringen till 24 § konstateras om teknisk avlyssning. I ett utrymme kan det vistas och röra sig också andra personer än personer som är föremål för ett underrättelseuppdrag. I dessa situationer ska information och upptagningar som gäller personer som inte är föremål för underrättelseuppdraget genast förstöras.

Optisk observation kan riktas mot en person eller grupp av personer som befinner sig i ett sådant hemfridsskyddat utrymme som avses i 24 kap. 11 § i strafflagen, förutsatt att utrymmet inte används för stadigvarande boende. Det har ingen betydelse var en teknisk anordning, metod eller programvara installeras, förutsatt att den optiska observationen inte inriktas på utrymmen som används för stadigvarande boende.

En förutsättning för användning är att metoden är av synnerlig vikt och det redogörs för detta i detaljmotiveringen till 20 §.

**27 §.** *Beslut om optisk observation.* I 1 mom. föreskrivs det på samma sätt som i fråga om teknisk avlyssning om optisk observation av en person som har berövats sin frihet. Beslut om denna typ av optisk observation ska fattas av domstol. I fråga om detta och brådskande beslut kan det hänvisas till detaljmotiveringen till 25 § 1 mom.

Beslut om annan optisk observation än optisk observation av en person som har berövats sin frihet ska enligt 2 mom. i den föreslagna paragrafen fattas av en med användningen av militärunderrättelsemyndighetens metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Enligt 3 mom. får tillstånd ges och beslut fattas för högst sex månader åt gången. I fråga om de faktorer som påverkar yrkandet och beslutsprövningen kan det hänvisas till vad som konstateras i detaljmotiveringen till 21 § 2 mom.

I 4 mom. i den föreslagna paragrafen räknas det upp vad som ska nämnas i ett beslut och detta överensstämmer med det som konstateras i detaljmotiveringen till 25 § 4 mom.

**28 §.** *Teknisk spårning.* I 1 mom. definieras begreppet teknisk spårning. Med *teknisk spårning* avses 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. Teknisk spårning är en av de mest traditionella metoderna för underrättelseinhämtning och denna metod ingriper inte i lika hög grad i en persons grundläggande fri- och rättigheter och mänskliga rättigheter som sådan teknisk spårning av en person som det föreskrivs om nedan.

Enligt momentet är det i princip möjligt att följa hur vilket som helst föremål eller ämne eller vilken som helst egendom förflyttas. I definitionen nämns spårning av förflyttningar till åtskillnad från andra former av optisk observation. Detta inbegriper naturligtvis också information om var föremål, ämnen eller egendom befinner sig när de inte är i rörelse.

Den tekniska spårningen kan utföras på ett teknikneutralt sätt med olika tekniska anordningar, metoder och programvaror. Vid teknisk spårning kan man t.ex. utnyttja ett föremåls, ett ämnes eller en egendoms existerande egenskaper som utvecklats för tekniska, kommersiella eller motsvarande ändamål eller på ett föremål, ett ämne eller en egendom fästa en teknisk anordning som möjliggör lokalisering eller i hemlighet installera programvara som möjliggör lokalisering. Som ett exempel kan nämnas hemlig aktivering av en lokaliseringsanordning som finns i ett motorfordon. Vid lokalisering av personer kan man använda t.ex. en spårningsanordning som göms i den persons kläder som ska spåras.

Enligt 2 mom. ska det kunna antas att man med teknisk spårning får information som är viktig med avseende på ett underrättelseuppdrag, såsom information om hur en enskild person förflyttar sig, eller information som underlättar observationen av en person. Information om föremålet för teknisk spårning kan ha fåtts t.ex. med andra metoder för underrättelseinhämtning.

I vissa fall kan den militära underrättelseinhämtningen inhämta information som är viktig med avseende på ett underrättelseuppdrag och som gäller t.ex. hur ett visst föremål förflyttar sig. Man kan i en viss situation identifiera ett föremål som lämpar sig för t.ex. militär verksamhet, men det kan ännu vara oklart vem som hanterar föremålet. Med teknisk spårning kan man följa hur föremålet förflyttar sig till en ny destination och efter detta med andra metoder för underrättelseinhämtning reda ut vem som är intresserade av föremålet.

Dessutom kan teknisk spårning riktas mot föremål, ämnen eller egendom, såsom en bil, som en sådan person som har samband med ett underrättelseuppdrag kan antas inneha eller använda. På detta sätt kan man direkt inhämta information om hur en viss person förflyttar sig, också om informationen inte är så exakt som den information som fås med teknisk spårning av en person enligt 3 mom.

I 3 mom. föreskrivs det särskilt om förutsättningarna för 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 personen bär eller i ett föremål som personen bär med sig, får åtgärden genomföras bara om detta med fog kan antas vara av synnerlig vikt för erhållande av

information med avseende på ett underrättelseuppdrag. I detaljmotiveringen till 20 § finns en redogörelse för denna förutsättning.

Information om att en person har samband med ett underrättelseuppdrag kan ha fåtts t.ex. med andra metoder för underrättelseinhämtning.

**29 §.** *Beslut om teknisk spårning.* Enligt 1 mom. ska beslut om teknisk spårning av en person fattas av domstol på yrkande av en av militärunderrättelsemyndigheterna för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Om ärendet inte tål uppskov, får beslut om teknisk spårning av en person fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman 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 från det att metoden för underrättelseinhämtning började användas.

Nedan föreskrivs det om situationer där domstolen i sin prövning ansett att förutsättningarna för sådan teknisk spårning av en person som påbörjats i ett brådskande förfarande inte har uppfyllts. I detta fall ska användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt samt anteckningarna om informationen genast förstöras.

Beslut om annan teknisk spårning än teknisk spårning av en person ska enligt 2 mom. fattas av en av militärunderrättelsemyndigheterna för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Enligt 3 mom. får tillstånd ges och beslut fattas för högst sex månader åt gången. Till denna del motsvarar bestämmelsen de övriga myndigheternas gällande befogenheter.

I 4 mom. föreskrivs det om vad som ska nämnas i ett yrkande och i ett beslut om teknisk spårning och detta motsvarar i huvudsak vad som föreskrivs om den information som ska nämnas i ett yrkande och i ett beslut som gäller andra metoder för underrättelseinhämtning, såsom konstateras i detaljmotiveringen till 25 §. Enligt 2 punkten ska i ett yrkande och i ett beslut nämnas det föremål, det ämne eller den egendom som åtgärden riktas mot och som spåras tekniskt.

**30 §.** *Teknisk observation av utrustning.* I 1 mom. definieras begreppet teknisk observation av utrustning. Med *teknisk observation av utrustning* avses t.ex. att en funktion, informationsinnehållet eller identifieringsuppgifterna i en dator eller i en annan 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 behövliga med avseende på ett underrättelseuppdrag. Teknisk observation av utrustning riktas mot t.ex. informationsutbyte mellan tekniska anordningar och programvaror samt till meddelanden som sparats i en elektronisk anordning.

Vid teknisk observation av utrustning har det ingen betydelse var en anordning används eftersom avsikten med befogenheten inte är att genom sinnesförnimmelser, dvs. med syn eller hörsel, utreda händelserna på platsen där anordningen finns. Teknisk observation av utrustning jämställs inte till denna del med de befogenheter som avses ovan.

Genom teknisk observation av utrustning iakttas en teknisk anordning och vanligen också den information som anordningen innehåller och som sparats av den person som har samband med underrättelseuppdraget. Sådan information kan finnas i dokument som har sparats i den tekniska anordningen. Teknisk observation av utrustning kan användas för att följa interaktionen

mellan en person och en teknisk anordning. Genom befogenheten är det möjligt att skaffa identifieringsuppgifter om en anordning eller dess programvara samt information om signal- eller styrtrafik som inte hör ihop med ett meddelande. Teknisk observation av utrustning kan användas för att följa interaktionen mellan en person och en teknisk anordning utan att öppna meddelanden. En form av teknisk observation av utrustning är s.k. tangentbordsavlyssning i syfte att ta reda på exempelvis ett lösenord till en nätserver. Åtgärden ska huvudsakligen vara av teknisk natur, till åtskillnad från observation som genom sinnesförnimmelser, dvs. med syn eller hörsel. I detaljmotiveringen till 24 § behandlas tangentbordsavlyssning för att ta reda på innehållet i ett meddelande.

I enlighet med definitionen kan inte vilken som helst teknisk anordning vara föremål för teknisk observation av utrustning, utan anordningen ska kunna jämställas med en dator, såsom smarttelefoner och s.k. pekdatorer.

I 2 mom. föreskrivs det om begränsningar av teknisk observation av utrustning. Av den gällande polislagen och motiveringen till den framgår det bara indirekt att med det innehåll i meddelanden som anges i bestämmelsen avses uttryckligen det innehåll i meddelanden som teleavlyssning och teknisk avlyssning riktar sig mot, dvs. när kommunikation sker mellan två människor i realtid via en dator eller smarttelefon eller telenätet i övrigt. Teknisk observation av utrustning omfattar således t.ex. de dokument som redan sparats i anordningen i fråga samt de meddelanden som inte är sådana meddelanden som håller på att skrivas och som teknisk avlyssning riktar sig mot eller de meddelanden som förmedlas och som teleavlyssning riktar sig mot, dvs. ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning och förmedlas genom ett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät eller någon annan kommunikationsförbindelse. Ett meddelande och dess innehåll kan också avse andra meddelanden än meddelanden som har överskridit ett kommunikationsnäts gränssnitt och som inte omfattas av det nämnda förbudet.

Den begränsning av teknisk observation av utrustning som nu behandlas innebär att den militära underrättelseinhämtningen med teknisk observation av utrustning kan inhämta information också om meddelanden i en teknisk anordning. Genom den nya bestämmelsen förtydligas också rättsläget i fråga om med utövande av vilken befogenhet man kan inhämta information om ett meddelande som har sparats i en teknisk anordning.

Föremål för utövande av befogenheten är alltid en viss person. Att befogenheten inte inbegriper meddelanden som förmedlas innebär att teknisk observation av utrustning inte kan användas t.ex. på ett system som används för förmedling av meddelanden så att den tekniska observationen av utrustning gäller alla meddelanden som förmedlas i systemet. På detta sätt förhindras det också att teleavlyssning och underrättelseinhämtning som avser datatrafik kringgås. Teknisk observation av utrustning får inte rikta sig mot meddelandetrafiken mellan personer och med teknisk observation av utrustning får det inte inhämtas information om innehållet i meddelande mellan personer eller om förmedlingsuppgifter. Detta framgår av uttrycket ”ett meddelande som förmedlas”.

Begränsningen av användningen av teknisk observation av utrustning avviker till de delar som beskrivs ovan från teknisk observation av utrustning enligt 5 kap. i den gällande polislagen. Den föreslagna ändringen kan anses motiverad också med anledning av tillämpningspraxis enligt 5 kap. i polislagen.

Teknisk observation av utrustning jämställs också med den kopieringsbefogenhet som föreslås nedan och enligt vilken kopiering kan riktas mot såväl handlingar och föremål som meddelan-

den. Med hjälp av teknisk observation av utrustning kan man inhämta information om t.ex. en statlig aktörs underrättelseverksamhet i Finland.

Genom momentet dras det en gräns mellan olika metoder för underrättelseinhämtning. Liksom det redan konstateras ovan anses t.ex. tangentbordsavlyssning för att ta reda på innehållet i ett meddelande medan meddelandet skrivs vara teknisk avlyssning. Efter det att ett meddelande har skickats och innan meddelandet har nått fram till mottagaren är det fråga om teleavlyssning.

Om det under pågående teknisk observation av utrustning framgår att observationen riktas mot innehållet i någon annans meddelande än det objekt som avses i tillståndet eller mot identifieringsuppgifter som gäller någon annans meddelande, ska användningen av denna metod för underrättelseinhämtning avbrytas så snart som möjligt och upptagningarna samt anteckningarna om den information som fåtts med hjälp av metoden omedelbart förstöras i fråga om andra än objektet, i enlighet med vad som föreskrivs nedan.

Genom utövandet av befogenheten ingriper man i skyddet för kommunikation. Vid teknisk observation av utrustning motsvarar beslutsfattandet vad som i 34 § föreskrivs om beslut om teleavlyssning och annat inhämtande av information. Tröskeln för användning av teknisk observation av utrustning kan således när det gäller förutsättningarna inte anses vara lägre än för andra metoder för underrättelseinhämtning som ingriper i kommunikation.

Med stöd av tillstånd till teknisk observation av utrustning kan den tjänsteman som utövar befogenheten samtidigt ha tillgång till också andra metoder för underrättelseinhämtning, om förutsättningarna för användningen av dem uppfylls.

Enligt 3 mom. kan militärunderrättelsemyndigheterna ges tillstånd till teknisk observation av utrustning hos en statlig aktör. Förutsättningen är i detta fall en allmän förutsättning för användning av metoder för underrättelseinhämtning.

I 4 mom. föreskrivs det om förutsättningarna för teknisk observation av utrustning hos andra än statliga aktörer. En förutsättning för teknisk observation av utrustning är att detta kan antas vara av synnerlig vikt för inhämtande av information med avseende på ett underrättelseuppdrag. Försvarsmaktens underrättelsetjänst får rikta teknisk observation av utrustning mot en dator eller en annan liknande teknisk anordning som en sådan person som har samband med ett underrättelseuppdrag sannolikt använder eller mot dess programvara.

Begränsningen enligt momentet till anordningar som används av en sådan person som har samband med ett underrättelseuppdrag innebär att anordningarna inte behöver ägas eller i övrigt innehas av personen i fråga. Föremål för underrättelseinhämtning kan också vara en anordning eller programvara som den person som är föremål för användning av en metod för underrättelseinhämtning ännu inte använder, men kommer att använda i framtiden. Beviströskeln för sambandet mellan en anordning och en misstänkt person är hög och ordet ”sannolikt” som används i momentet hänvisar till detta. Om det i samband med användningen av en metod för underrättelseinhämtning observeras att en teknisk anordning används av någon annan än den person som metoden riktar sig mot ska åtgärden avbrytas samt eventuella upptagningar och anteckningar om information som fåtts genom åtgärden förstöras.

Det redogörs i detaljmotiveringen till 20 § för den särskilda förutsättning att metoden är av ”synnerligen stor betydelse” som är en förutsättning för användning.

**31 §.** *Beslut om teknisk observation av utrustning.* Enligt 1 mom. ska beslut om teknisk observation av utrustning fattas av domstol på yrkande av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vid en militärunderrättelsemyndighet. Om ärendet inte tål uppskov, får beslut om spårning fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vid en militärunderrättelsemyndighet till dess 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 för underrättelseinhämtning började användas.

Nedan föreskrivs det om situationer där domstolen i sin prövning ansett att förutsättningarna för sådan teknisk spårning av en person som påbörjats i ett brådskande förfarande inte har uppfyllts. I detta fall ska användningen av en metod för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om den information som fåtts på detta sätt genast utplånas.

Som ett undantag från övriga myndigheters gällande metoder för hemlig informationsinhämtning omfattar den tekniska observation av utrustning som behandlas i denna proposition även ingripande i skyddet för meddelanden. Beslutsfattandet och förutsättningarna för användning av teknisk observation av utrustning motsvarar dock övriga metoder för underrättelseinhämtning som ingriper i skyddet för meddelanden och förutsätter tillstånd av domstol.

Enligt 2 mom. får tillstånd ges och beslut fattas för högst sex månader åt gången. Till denna del motsvarar bestämmelsen de övriga myndigheternas gällande befogenheter. Den maximala tiden på sex månader har motiverats ovan.

I 3 mom. finns uppräknade de omständigheter som ska nämnas i ett yrkande och i ett beslut. Momentet motsvarar de krav som ovan föreskrivs för användning av metoder för underrättelseinhämtning. De omständigheter som ska nämnas i yrkandet och beslutet beskrivs närmare ovan i detaljmotiveringen till 25 §.

**32 §.** *Teleavlyssning.* I paragrafen föreskrivs om teleavlyssning. Enligt 1 mom. avses med teleavlyssning att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och identifieringsuppgifterna i anslutning till det. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som har en ytterst stor betydelse för ett underrättelseuppdrag.

Vid teleavlyssning är det fråga om att avlyssna meddelanden huvudsakligen i de allmänna kommunikationsnäten.

I momentet ingår som ett särskilt nämnt undantag i fråga om gällande lagstiftning om befogenheter, t.ex. teleavlyssning som avses i 5 kap. i polislagen, även meddelanden som förmedlats till en viss teleadress eller teleterminalutrustning genom någon annan meddelandeförbindelse. Med annan förbindelse avses t.ex. samtal och meddelanden som förmedlas i ett satellitnätverk samt andra sådana former för att förmedla meddelanden som eventuellt kommer att utvecklas i framtiden.

Vid satellitsamtal används en satellitförbindelse i stället för basstationer på marken, och det kan inte anses att detta omfattas av definitionen av allmänt kommunikationsnät. Det är motiverat att beakta satellitnätverket därför att antalet satelliter ökar, deras storlek minskar i och

med den tekniska utvecklingen och det blir allt lättare att skicka upp dem. Ett satellitnätverk är i allmänhet uppbyggt av tre delar, och det består av en rymddel (satellit), markstationer och rörliga stationer, dvs. exempelvis telefoner. När det gäller markstationer bör man dessutom observera att endast de sändande markstationerna kräver tillstånd av Kommunikationsverket, medan mottagande markstationer inte kräver tillstånd.

Teleavlyssning som riktas mot satellittelefoner har ofta förutsatt att en begäran om handräckning har lämnats till den stat som äger markstationen, men informationsinhämtningen kan med stöd av den föreslagna bestämmelsen även riktas direkt till t.ex. förbindelsen mellan en satellittelefon och en markstation.

Annan meddelandeförbindelse täcker även sådana situationer där teleavlyssning t.ex. vid sådan militär underrättelseinhämtning som genomförs utomlands genomförs med hjälp av en militärunderrättelsemyndighets falska basstation. I situationer av detta slag tar den teleterminalutrustning eller den teleadress som föremålet för underrättelseinhämtningen använder kontakt med militärunderrättelsemyndighetens falska basstation utan att föremålet vet om detta, och därifrån flyttas kommunikationen över till det lokala kommunikationsnätet. Definitionen i 5 kap. 5 § i polislagen kan inte anses omfatta ovan beskrivna situation, eftersom det i detta skede inte ännu är fråga om ett meddelande som förmedlas i det allmänna kommunikationsnätet.

Teleavlyssningen inriktas så att den grundar sig på gränssnittsinformation i ett kommunikationsnät eller någon annan kommunikationsförbindelse eller på en egenskap som kan sammankopplas med en viss användare eller abonnent och på den information eller egenskap som ingår i utrustningen och därmed också kan sammankopplas med användaren eller abonnenten. Information av detta slag kan bestå av t.ex. e-postadresser, IP-adresser, användarnamn och lösenord, profiler eller annan information i telenätet, med hjälp av vilka parterna i tele- eller datakommunikation kan identifieras. Definitionen av begreppet teleavlyssning inbegriper sålunda också telefoners serienummer (IMEI-kod) eller annan information som direkt identifierar en terminalutrustning eller leder till att den kan identifieras.

Med meddelande avses enligt lagen om tjänster inom elektronisk kommunikation samtal, elektronisk post, textmeddelanden, talmeddelanden och andra motsvarande meddelanden som i ett kommunikationsnät förmedlas mellan parterna eller till en mottagarkrets som inte är utvald på förhand. Begreppet omfattar så gott som alla former av information, dock inte sådan styr- och signaltrafik mellan datorer som inte har något samband med meddelandet. Befogenhet att använda teleavlyssning behövs inte för utredning av innehållet i nätkommunikation som är tillgänglig för alla. Data som gör det möjligt att identifiera nätmeddelanden är emellertid konfidentiella, vilket också motsvarar gällande rätt. Teleavlyssning avser meddelanden som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning. Den som har befogenhet för avlyssning kan komma åt meddelandet när det förmedlas i kommunikationsnätet på ett sådant sätt att meddelandet har passerat t.ex. den avsändande teleadressens gränssnitt och sålunda blivit avsänt, men har inte passerat den mottagande teleadressens gränssnitt och kan således fortfarande tas emot. Detta innebär att sedan t.ex. ett textmeddelande anlänt till en mobiltelefon förmedlas det inte längre i den bemärkelse som avses här.

En befogenhet för teleavlyssning inbegriper inhämtande av information om förmedling av ett meddelande. Ett meddelande utan tillhörande identifieringsuppgifter (t.ex. om avsändaren och mottagaren) är i praktiken betydelselöst. Till denna del ingår teleövervakning i teleavlyssning. Genom en befogenhet för teleavlyssning kan det dock inte t.ex. förhindras att ett meddelande når mottagaren. Identifieringsuppgifter som erhålls i samband med teleavlyssning innehåller

inte heller information om var teleterminalutrustningen är belägen. Detta avses när det uttryckligen nämns att de identifieringsuppgifter som hänför sig till ett meddelande ska utredas. Om också information om var utrustningen är belägen behövs, måste ett tillstånd till teleövervakning skaffas. I momentet konstateras uttryckligen att teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas ha samband med ett underrättelseuppdrag eller vars mottagare är en sådan person som med fog kan antas ha samband med ett underrättelseuppdrag och om den information som inhämtas är av synnerlig vikt med avseende på ett underrättelseuppdrag. Avsikten med detta är att understryka att teleavlyssning inte får riktas mot någon annan än en nämnd persons meddelanden. Denne kan visserligen vara en person som ännu är okänd och som med fog kan antas vara väsentlig med avseende på ett underrättelseuppdrag. Personen kan då identifieras med hjälp av en teleadress eller teleterminalutrustning som denne innehar eller annars kan tänkas använda. Det måste dock uttryckligen ses till att beviljande av avlyssningstillstånd för teleadresser eller teleterminalutrustningar som används av okända personer inte de facto leder till avlyssning av vissa teleadresser eller teleterminalutrustningar, oberoende av vem som använder dem.

Såsom det i det inledande stycket till detaljmotiveringen till 4 kap. har konstaterats får befogenhet för teleavlyssning användas endast vid sådan informationsinhämtning där ett underrättelseuppdrag grundar sig på föremålet för militär underrättelseinhämtning eller som är militär verksamhet eller som utgör ett allvarligt hot för den nationella säkerheten i Finland. Dessutom ska man fästa vikt vid huruvida föremålet för informationsinhämtningen är en statlig aktör eller någon annan aktör. Exempelvis i 4 § 1 mom. avsedd verksamhet som till sin art är militär åtnjuter inte skydd enligt 10 § 2 mom. i grundlagen, och genom teleavlyssning som riktas mot kommunikation mellan personer som deltar i sådan verksamhet ingriper man inte i skyddet för konfidentiell kommunikation.

På motsvarande sätt fastställs i 4 § 1 mom. 2 punkten att föremålet för den militära underrättelseinhämtningen är inhämtande av information om utländska underrättelsetjänsters underrättelseverksamhet som riktar sig mot Finlands försvar. Såsom ovan har konstaterats åtnjuter statliga aktörer inte skydd för de grundläggande fri- och rättigheterna, och detta innebär att kommunikation mellan företrädare för identifierade utländska underrättelsetjänster inte åtnjuter skydd i Finland.

I momentet föreskrivs det uttryckligen att teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas ha samband med ett underrättelseuppdrag. Med detta vill man framhäva att teleavlyssning inte får riktas mot någon annan persons kommunikation. Personen kan vara en för militärunderrättelsemyndigheten okänd person som med fog kan antas t.ex. förmedla information för militärunderrättelsen i en främmande stat. Personen kan då identifieras med hjälp av en teleadress eller teleterminalutrustning som denne innehar eller annars kan tänkas använda. Man måste dock särskilt se till att om någon annan än en person som har stor betydelse för ett underrättelseuppdrag använder en obekant teleadress eller teleterminalutrustning, ska den inhämtade informationen omedelbart utplånas när det framkommer att föremålet för användningen av en metod för underrättelseinhämtning inte var en person som är väsentlig med avseende på underrättelseuppdraget.

En viss teleadress, teleterminalutrustning eller person som är föremål för teleavlyssning kan kommunicera även med personer som inte har något samband med den verksamhet som är föremål för underrättelseuppdraget. Om kommunikation som inte har något samband med ett underrättelseuppdrag blir föremål för informationsinhämtning vid teleavlyssning måste kommunikationen utplånas omedelbart. Bestämmelser om utplåning av information finns i 7 kap.

Enligt 2 mom. i paragrafen får teleavlyssning riktas mot en statlig aktör när de allmänna förutsättningarna för underrättelsemetoder uppfylls.

En förutsättning för att denna befogenhet ska få användas är tillstånd av en domstol. Bestämmelser om detta finns i 33 §. Såsom det ovan har konstaterats i den allmänna motiveringen till denna proposition, kan en statlig aktör inte anses åtnjuta skydd för grundläggande fri- och rättigheter. Kommunikation mellan två statliga aktörer omfattas således inte av sekretessen för konfidentiella meddelanden. Det är skäl att observera att teleavlyssning får riktas endast mot kommunikation som sker internt inom en statlig aktör eller mellan statliga aktörer. All annan kommunikation ska utplånas, såsom det föreskrivs nedan i denna proposition. Teleavlyssningen måste riktas mot en person som företräder en statlig aktör och som är väsentlig med avseende på underrättelseuppdraget. Detta krav innebär att en militärunderrättelsemyndighet på förhand har en uppfattning om att den person som kommer att bli föremål för teleavlyssning företräder en statlig aktör.

Teleavlyssning av en statlig aktör kan komma på fråga t.ex. i situationer där en person som företräder en underrättelsetjänst från en främmande makt har identifierats.

Anmärkningsvärt är även det att föremålet för användningen av metoder för underrättelseinhämtning till en början med stöd av befintlig information kan framstå som någon annan än en statlig aktör, men i och med att underrättelseverksamheten framskrider kan det framkomma att personen i fråga t.ex. är företrädare för en underrättelseorganisation från en främmande makt eller att personen direkt styrs av en statlig aktör.

I paragrafens 3 mom. föreskrivs det om teleavlyssning av någon annan än en statlig aktör. En förutsättning för att denna befogenhet ska få användas är tillstånd av en domstol. Bestämmelser om detta finns i 33 §.

Föremål för teleavlyssning kan vara en person som med fog kan antas ha samband med ett underrättelseuppdrag. För att metoder för underrättelseinhämtning ska få användas är att underrättelseinhämtningen är av synnerlig vikt för inhämtandet av information med avseende på underrättelseuppdraget. Kravet beskrivs närmare ovan i detaljmotiveringen till 20 §. Föremålen för militär underrättelseinhämtning strävar efter att hemlighålla de verkliga ändamålen med sin verksamhet och att verka i det fördolda. Detta kan komma på fråga t.ex. när information ska inhämtas om en främmande makts underrättelseverksamhet och den person eller grupp av personer som är föremål för underrättelseinhämtningsmetoden inte kan identifieras som en statlig aktör, utan det är t.ex. fråga om en aktör som omedvetet förmedlar information till en sådan aktör eller om en person som till en främmande makts aktör förmedlar information som skadar Finlands försvar.

**33 §.** *Inhämtande av information i stället för teleavlyssning.* I 1 mom. finns bestämmelser om vissa metoder för inhämtande av information av samma slag som teleavlyssning. Enligt 1 mom. kan militärunderrättelsemyndigheterna, om det är sannolikt att ett meddelande som avses i 32 § och dess identifieringsuppgifter inte längre är tillgängliga genom teleavlyssning, beviljas tillstånd att inhämta informationen hos ett teleföretag eller en sammanslutningsabonnent under de förutsättningar som anges i 32 §. En förutsättning för en underrättelseinhämtningsmetod är också att den kan antas vara av synnerlig vikt för genomförandet av ett underrättelseuppdrag.

I paragrafen är det fråga om sådana fall där ett meddelande som har erhållits genom en befogenhet för teleavlyssning har försvunnit, men meddelandet finns ännu tekniskt tillgängligt hos

teleföretaget eller sammanslutningsabonnenten. Syftet med bestämmelserna är också att förhindra att förutsättningarna för användning av teleavlyssning kringgås. För att en åtgärd ska få användas ställs som villkor sannolikheten för att meddelandet och därtill hörande förmedlingsuppgifter inte längre finns tillgängliga genom teleavlyssning.

De situationer som avses i momentet kommer på fråga när man vet att det redan innan teleavlyssningen inleds finns information som kan användas för underrättelseuppdraget. Dessa förutsättningar motsvarar teleavlyssning.

Enligt 2 mom. kan militärunderrättelsemyndigheten, 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, beviljas tillstånd till inhämtande av information i stället för teleavlyssning, om de förutsättningar som anges i 32 § finns. Detta förhindrar att tröskeln för att tillämpa teleavlyssning blir lägre än normalt när avlyssningen kan genomföras genom t.ex. observation på teknisk väg av sådan personlig tilläggsutrustning som används vid förmedling av samtal, nämligen handsfree eller någon annan anordning i anslutning till t.ex. mobiltelefonen genom Bluetooth. Föremålet för användningen av metoder för underrättelseinhämtning kan i ovannämnda situationer med fog anta att kommunikationen är lika konfidentiell som när man talar direkt i mobiltelefonen.

Enligt momentet utförs inhämtandet av information i stället för teleavlyssning för att utreda innehållet i ett meddelande. Anordningen ska finnas i omedelbar anslutning till den tekniska anordningen, och detta innebär att olika mobila lagringsmedier utesluts. De anordningar som avses i momentet ska uttryckligen vara sådana personliga hjälpmedel som lämpar sig för sändande och mottagande av meddelanden eller andra motsvarande tekniska anordningar. Här är det dock fråga om teknikneutrala bestämmelser.

Enligt momentet ska inhämtandet av information riktas mot förbindelsen mellan en personlig teknisk anordning och en teleterminalutrustning. I detta fall riktar sig inhämtandet av information inte till hjälpmedlet utan till radioförbindelsen eller någon annan motsvarande förbindelse mellan hjälpmedlet och teleterminalutrustningen. Avlyssning av t.ex. ett samtal via mobiltelefonens högtalare eller ett högljutt samtal är inte sådant inhämtande av information i stället för teleavlyssning som avses i momentet.

**34 §.** *Beslut om teleavlyssning och annat motsvarande inhämtande av information.* Enligt 1 mom. ska beslut om teleavlyssning och om inhämtande av information i stället för teleavlyssning fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Nedan i 113 § föreskrivs det om behandling av yrkandet i domstol.

Enligt första meningen i 2 mom. får tillstånd till teleavlyssning eller inhämtande av information i stället för teleavlyssning ges för högst sex månader åt gången. Tiden för ett gällande tillstånd är längre än vad som anges i gällande lagstiftning, t.ex. i fråga om teleavlyssning som avses i 5 kap. i polislagen. Detta är motiverat med avseende på karaktären hos och uppgifterna för militär underrättelseverksamhet, grunderna för användning av metoder för underrättelseinhämtning och användningsändamålet. Underrättelseverksamhetens karaktär avviker avsevärt från brottsbekämpningens behov. Om en förlängning av användningen av underrättelseinhämtningsmetoder behövs efter dessa sex månader, ger en ny behandling även domstolen en ny möjlighet att kontrollera att förutsättningarna för tillståndet fortfarande finns utan att rättsskyddet äventyras.

Med hjälp av befogenheten för teleavlyssning är det möjligt att få ytterst exakt och omfattande information om en enskild persons verksamhet. När det gäller underrättelseverksamhet får information som inhämtats vid teleavlyssning dock inte användas vid brottsbekämpning. Ett undantag från denna huvudregel är dock 6 kap., där det ingår noggranna bestämmelser om sådana situationer då information som inhämtats genom underrättelseinhämtningsmetoder får lämnas ut till andra än den militära underrättelseinhämtningen.

Såsom det ovan har konstaterats angående teknisk avlyssning är underrättelseinhämtning långsiktig och på förhand välplanerad verksamhet. Avsikten med underrättelseinhämtning är inte att förhindra eller reda ut ett enskilt brott utan att samla in information i ett tidigt skede för att få en helhetsbild. Bestämmelsen möjliggör att man med ett enda tillståndsbeslut kan utföra förutseende och mer långvarigt inhämtande av information.

Enligt den andra meningen i 2 mom. får tillstånd ges för högst tre månader åt gången när åtgärden gäller en person. Vid teleavlyssning (och teleövervakning) kan föremålet för en åtgärd med avvikelse från gällande lagstiftning utöver en teleadress eller teleterminalutrustning även vara en person. I ett förfarande av detta slag skulle det vara motiverat att iaktta en kortare tillståndstid. Om en förlängning behövs för användning av teleavlyssning efter tre månader, ger en ny behandling även domstolen en genuin möjlighet att kontrollera inriktandet av teleavlyssningen.

Om den teleterminalutrustning eller den teleadress som används av en person som är föremål för teleavlyssning har hamnat hos någon annan användare, måste teleavlyssningen avbrytas till denna del och den information som inhämtats efter detta utplånas i enlighet med 82 §.

I 3 mom. föreskrivs om den information som ska ingå i ett yrkande och i ett beslut.

I momentets 1 punkt avses med det underrättelseuppdrag som ligger till grund för åtgärden ett underrättelseuppdrag enligt 9 § 6 punkten som grundar sig på föremål för den militära underrättelseinhämtningen enligt 4 § och på en begäran om information enligt 13 §. Ett underrättelseuppdrag ska ligga till grund för användningen av en metod för underrättelseinhämtning. Av yrkandet och beslutet ska dessutom framgå syftet med åtgärden, dvs. vad som eftersträvas med användningen av en metod för underrättelseinhämtning. Syftet med användningen av befogenheten ska fastställas med tillräcklig noggrannhet.

I momentets 2 punkt föreskrivs om förutsättningen att i yrkandet och beslutet införa det föremål för en metod för underrättelseinhämtning som vid teleavlyssning är en teleadress eller en teleterminalutrustning eller en person.

Enligt denna punkt kan teleavlyssningen även riktas mot en person. När tillståndet till teleavlyssning gäller en person innefattar tillståndet även den teleadress eller den teleterminalutrustning som den person som är föremål för teleavlyssningstillståndet innehar eller kan tänkas använda. Teleavlyssningstillståndet gäller inte för en enskild teleadress eller teleterminalutrustning, utan tillståndet gäller alla teleadresser och teleterminalutrustningar som den person som tillståndet gäller innehar. Tillståndssökanden ska kunna visa grunderna för att en viss teleadress eller teleterminalutrustning innehas av den person som tillståndet gäller eller att personen annars kan tänkas använda teleadressen eller teleterminalutrustningen. Vid teleavlyssning som riktas mot en person kan inhämtandet av information utgöra ett komplement till andra metoder för underrättelseinhämtning, t.ex. inhämtande av identifieringsuppgifter för en teleadress eller teleterminalutrustning. När en i domstolens tillstånd fastställd person som är föremål för en åtgärd börjar använda eller antas ha börjat använda nya teleadresser eller ny tele-

terminalutrustning eller när det framkommer att denne innehar en teleadress eller teleterminalutrustning som inte redan har specificerats i den tillståndsansökan som tillställts domstolen, kan underrättelsemyndigheten rikta åtgärden mot dessa. Även vad gäller dessa teleadresser eller denna teleterminalutrustning ska anmälan göras hos underrättelseombudsmannen.

Vid teleavlyssning som riktas mot en person bör man beakta personens ställning som statlig aktör eller som någon annan aktör.

Momentets 3 punkt är av betydelse med avseende på beslutsfattandet. Enligt punkten ska i ett yrkande och i ett beslut tas in de fakta som förutsättningarna för och inriktningen av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning grundar sig på. Framläggandet av fakta för domstolen ålägger underrättelsemyndigheten att lägga fram och motivera de fakta på basis av vilka domstolen har en faktisk möjlighet till omsorgsfull tillståndsprövning, och domstolen kan dra sina egna slutsatser av huruvida förutsättningarna för användning av en underrättelseinhämtningsmetod uppfylls. Vad gäller de nämnda förutsättningarna är det fråga om allmänna förutsättningar för metoder för underrättelseinhämtning enligt 11 § och om de förutsättningar som nämns i 32 §, som gäller befogenhet. I ett yrkande och i ett beslut ska vidare läggas fram tillräckliga fakta om underrättelseuppdraget och om det i 4 § avsedda föremålet för militär underrättelseinhämtning samt om den i 13 § avsedda begäran om information eller om något annat av försvarsmaktens interna uppdrag. När tillstånd söks och beslut motiveras är de allmänna principerna för militär underrättelseinhämtning särskilt viktiga. Med tanke på proportionalitetsprincipen är det särskilt viktigt hur allvarlig verksamheten i fråga är.

Den information som avses i punkten ska vara tillräcklig och korrekt till innehållet. Domstolen kan försäkra sig om att informationen är tillräcklig genom att använda sin frågerätt. När sökanden lägger fram sakförhållandena handlar denne dessutom under tjänsteansvar och svarar för att de grunder som läggs fram är korrekta.

Domstolens prövning kan grunda sig enbart på det faktum att sökanden - trots ärendenas höga sekretessgrad - öppet och korrekt redogör för domstolen om den verksamhet som man vill inhämta information om genom att använda metoder för underrättelseinhämtning samt om föremålet för åtgärden.

Enligt momentets 4 punkt ska det i ett yrkande och i ett beslut nämnas giltighetstiden med angivande av klockslaget för tillståndet till teleavlyssning eller inhämtande av information i stället för teleavlyssning. Angivande av klockslaget förutsätts inte vid inhämtande av information i stället för teleavlyssning.

Enligt momentets 5 punkt ska det i ett yrkande och i ett beslut nämnas den tjänsteman vid Försvarsmaktens underrättelsetjänst som leder och övervakar utförandet av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.

Enligt momentets 6 punkt ska det i ett yrkande eller i ett beslut nämnas eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning. Domstolen kan i sitt beslut uppställa begränsningar och användarvillkor för teleavlyssning. Om man känner till sådana begränsningar och villkor redan när yrkandet uppgörs, ska den som framställer yrkandet överväga om de ska skrivas in i yrkandet.

**35 §.** *Teleövervakning.* Enligt 1 mom. avses med *teleövervakning* att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som

är kopplad till ett kommunikationsnät 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 som kan förknippas med en abonnent eller användare och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. Identifieringsuppgifterna definieras i 9 §.

Enligt 136 § i lagen om tjänster inom elektronisk kommunikation är förmedlingsuppgifter som hänför sig till ett meddelande konfidentiella, om inte något annat föreskrivs i lag. Ett meddelande är inte konfidentiellt om det är föremål för allmän mottagning. I 17 § i lagen om yttrandefrihet i masskommunikation föreskrivs om utlämnande av identifieringsuppgifter för ett nätmeddelande, dvs. information, åsikter eller andra meddelanden som gjorts tillgängliga för allmänheten genom radiovågor, elektroniska kommunikationsnät eller annan motsvarande teknik.

Vid användning av identifieringsuppgifter är det i allmänhet fråga om utredning av kommunikationsparter.

Identifieringsuppgifter kan omfatta uppgifter som bland annat anger vilken väg kommunikation routas, dess varaktighet, tidpunkt, eller mängden överförd data, det använda protokollet, den position där avsändarens eller mottagarens teleterminalutrustning befinner sig på en viss basstations område, det avsändande och mottagande nätet samt kommunikationens början, slut och varaktighet. Uppgifterna kan också avse den form i vilken meddelandet förmedlas i nätet. Den avgörande faktorn är att uppgifterna ska kunna förknippas med en abonnent eller användare. Som exempel kan nämnas e-postmeddelanden, vars identifieringsuppgifter är de rubrikuppgifter i meddelandet som gäller avsändare, mottagare, ruttinformation och tidsangivelser. I fråga om begreppet identifieringsuppgift bör det beaktas att den abonnent till vilken identifieringsuppgifterna kan kopplas kan vara såväl en fysisk som en juridisk person. Dessutom måste det beaktas att man med hjälp av teleövervakning kan få identifieringsuppgifter om telemeddelanden, men rätten att få identifieringsuppgifter innebär inte rätt till teleavlyssning. Information om meddelandets innehåll kan inte skaffas med denna befogenhet. Teleövervakning omfattar också inhämtande av information om teleadressers och teleterminalutrustningars position.

Bestämmelsen är teknikneutral. På grund av den tekniska utvecklingen kan den utrustning som används för kommunikation variera mycket. Det är inte alltid ens klart om det är fråga om mobilteleapparater eller utrustning av samma slag som mobilteleapparater. Den föreslagna definitionen innefattar över huvud taget inhämtande av information om alla typer av mobila teleadressers och teleterminalutrustningars position, oberoende av om det är fråga om en mobilteleapparat.

Den militära underrättelseverksamheten kan inhämta information om t.ex. var den person som är föremål för underrättelseuppdraget rör sig och vem denna person kommunicerar med.

Begränsningen av definitionen till uppgifter om ett meddelande innebär att sådan styrningstrafik mellan datorer som inte har samband med ett meddelande inte omfattas av skyddet för konfidentiell kommunikation. Med styrningstrafik avses information som på nätet hänför sig till informationsöverföring, dvs. att information flyttas från en viss teknisk utrustning till en viss avsedd teknisk utrustning. Denna information kan inhämtas med en befogenhet som gäller teknisk observation av utrustning.

Enligt 2 mom. kan militärunderrättelsemyndigheterna på samma sätt som i fråga om teleavlyssning ges tillstånd till teleövervakning av en sådan teleadress eller teleterminalutrustning som en statlig aktör använder och som är viktig för utförande av ett underrättelseuppdrag. Som det framgår av detaljmotiveringen till teleavlyssning åtnjuter statliga aktörer inte skydd av grundläggande fri- och rättigheter på samma nivå som privatpersoner.

På motsvarande sätt som i fråga om teleavlyssning kan teleövervakning enligt 3 mom. inriktas mot någon annan än en statlig aktör. Teleövervakning kan i dessa fall användas under stramare förutsättningar, dvs. om teleövervakningen kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

**36 §.** *Beslut om teleövervakning.* Enligt 1 mom. ska beslut om teleövervakning fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Om ett ärende som gäller teleövervakning inte tål uppskov, får beslut om teleövervakning fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vid militärunderrättelsemyndigheten till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar från det att metoden började användas.

Om domstolen i samband med ett beslut som fattats i en brådskande situation anser att det inte funnits förutsättningar för åtgärden, måste användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om den information som fåtts på detta sätt omedelbart utplånas.

Ett brådskande ärende gällande ett beslut ska föras till domstol också i det fall att användningen av teleövervakning avslutas inom 24 timmar efter att den påbörjades. I annat fall skulle man genom helt kortvarig informationsinhämtning kunna kringgå de krav som ställs på beslutsförfarandet. Att även i sådana fall föra ärendet till domstol främjar lagenligheten i verksamheten. Detta gäller även andra situationer där en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller någon annan tjänsteman vid Försvarsmaktens underrättelsetjänst temporärt kan besluta om användning av underrättelseinhämtningsmetoder.

Den beslutanderätt som avses i momentet motsvarar delvis bestämmelserna i 5 kap. 10 § 1 och 2 mom. i gällande polislag. Om en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller någon annan tjänsteman i en brådskande situation har fattat beslut och domstolen anser att det inte funnits förutsättningar för åtgärden, måste användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om den information som fåtts på detta sätt omedelbart utplånas.

I 2 mom. föreskrivs om teleövervakning som grundar sig på samtycke. Militärunderrättelsemyndigheterna får för inhämtande av information med avseende på ett underrättelseuppdrag med en persons samtycke rikta teleövervakning mot en teleadress eller teleterminalutrustning som denne innehar, om detta med fog kan antas vara av synnerlig vikt för inhämtandet av information om den verksamhet som är föremål för den militära underrättelseinhämtningen. Om exempelvis en person blir indragen i ett underrättelseuppdrag när denne omedvetet förmedlar information till underrättelsetjänsten i en främmande stat och om en militärunderrättelsemyndighet får kännedom om detta, kan militärunderrättelsemyndigheten inleda samarbete med

personen i fråga för att reda ut situationen och personen i fråga kan ge sitt samtycke till teleövervakning av sin egen teleterminalutrustning eller teleadress.

Med innehav av en teleadress eller teleterminalutrustning avses faktiskt innehav. Sålunda kan t.ex. en arbetsgivare inte ge samtycke till teleövervakning av en mobiltelefon som används av en arbetstagare. Inte heller tillfällig användning av en annan persons mobiltelefon kan berättiga till att samtycke ges till teleövervakning av telefonägarens kommunikation. Samtycket ska alltid ges i skriftlig form. I brådskande situationer kan samtycke dock ges muntligen, men det ska så snart som möjligt bekräftas skriftligen (RP 224/2010 rd., s. 103-104).

Enligt den rådande uppfattningen i doktrinen om den kränktes samtycke kan var och en på ett giltigt sätt ge sitt samtycke till teleövervakning av en teleadress eller teleterminalutrustning som denne har i sin besittning, om samtycket ges frivilligt före åtgärden och den som ger samtycket insett dess betydelse. Samtycket ska vara genuint frivilligt. Militärunderrättelsemyndigheten får inte utöva påtryckning eller på annat sätt ställa ledande frågor för att få samtycket. Militärunderrättelsemyndigheten kan nämna möjligheten att använda samtyckesbaserad teleövervakning, men vederbörande 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 beslut om den teleövervakning som avses i 2 mom. fattas av Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

I frågor som gäller militär underrättelseinhämtning finns beslutanderätten i fråga om teleövervakning som kräver samtycke alltid hos Huvudstabens underrättelsechef eller hos en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vid Försvarsmaktens underrättelsetjänst.

Enligt 4 mom. får tillstånd beviljas och beslut fattas för högst sex månader åt gången. Tillstånd kan ges även för en viss tid före beslutet fattades, vilken kan vara längre än sex månader. De uppgifter som gäller tiden före beslutet fattades är sådana uppgifter som teleföretaget bevarar, och bestämmelser om lagring av dessa uppgifter och om lagringstider finns i 157 § i lagen om tjänster inom elektronisk kommunikation. Förvaringstiden är som mest 12 månader. Detta innebär att tillstånd för retroaktiv teleövervakning kan ges för högst 12 månader.

När det gäller retroaktiv teleövervakning måste det noggrant överläggas hur lång tid tillståndet ska gälla. I underrättelseinhämtningssyfte är det genom retroaktiv teleövervakning möjligt att i mycket stor omfattning få information om vem eller vilka en viss aktör har haft kontakt med.

I 5 mom. föreskrivs vad som ska nämnas i ett yrkande och i ett beslut om teleövervakning. I fråga om detta kan det hänvisas till det som framförs i detaljmotiveringen till 34 § 3 mom.

**37 §.** *Inhämtande av basstationsuppgifter.* I 1 mom. avses med *inhämtande av basstationsuppgifter* inhämtande av information om teleterminalutrustningar och teleadresser som redan är eller kommer att bli registrerade i ett telesystem via en viss basstation. Inhämtande av basstationsuppgifter vid militär underrättelseinhämtning riktar sig mot en på förhand ospecificerad grupp teleadresser och teleterminalutrustningar, t.ex. mobilteleapparater. Befogenheten berättigar till inhämtande av uppgifter endast om en mobilteleapparats position vid en viss tidpunkt, men däremot inte uppgifter om huruvida den har tagit kontakt med någon annan mobilteleapparat. Genom användning av befogenheten kan man utreda både vilken teleterminalutrustning och vilka basstationer som redan tidigare har registrerats på en basstation och vilka

teleadresser och vilken teleterminalutrustning som registrerats på en viss basstation under den tid tillståndet har varit giltigt. Genom metoder för underrättelseinhämtning kan information inhämtas om en viss teleterminalutrustnings eller teleadress rörelser. Det är inte fråga om en metod som på ett lika betydande sätt ingriper i skyddet av de grundläggande fri- och rättigheterna som teleavlyssning, och metoden för underrättelseinhämtning jämställs med teknisk spårning.

Enligt 2 mom. kan militärunderrättelsemyndigheterna beviljas tillstånd att inhämta basstationsuppgifter, om det genom detta är möjligt att få sådan information om de personer som rör sig i ett utrymme eller på ett område som, när de allmänna förutsättningarna uppfylls, med avseende på underrättelseuppdraget är nödvändig. Väsentlig information för utförandet av ett underrättelseuppdrag kan fås genom att information inhämtas om vilka som rör sig på ett visst område eller i ett visst utrymme. I detta syfte vore det effektivt att inhämta basstationsuppgifter. Av teleadressens och teleterminalutrustningens registreringsuppgifter är det dock inte möjligt att direkt få information om enskilda personers rörelser på ett visst område, utan informationen om teleadresserna och teleterminalutrustningarna måste separat kopplas till en enskild person med andra medel.

**38 §.** *Beslut om inhämtande av basstationsuppgifter.* Enligt 1 mom. ska beslut om inhämtande av basstationsuppgifter fattas av domstol på yrkande av en sådan tjänsteman vid en militärunderrättelsemyndighet som är särskilt utbildad för användningen av metoder för underrättelseinhämtning. Om ärendet inte tål uppskov, får beslut om inhämtande av basstationsuppgifter fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman till dess 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 för underrättelseinhämtning började användas.

Inhämtande av basstationsuppgifter innebär lindrigare ingrepp i de grundläggande fri- och rättigheterna än vad teleövervakning gör, och det ingriper inte i skyddet för konfidentiell kommunikation. Om beslut om inhämtande av basstationsuppgifter har fattats i en brådskande situation och domstolen anser att det inte funnits förutsättningar för åtgärden, måste användningen av metoden för underrättelseinhämtning avslutas och det material som fåtts på detta sätt och anteckningarna om den information som fåtts på detta sätt omedelbart utplånas. Jämfört med de befogenheter som avser utredning av brott får information som fåtts genom en metod för underrättelseinhämtning inte användas som överskottsinformation.

Enligt 2 mom. beviljas tillstånd för en viss tidsperiod. Momentet motsvarar i sak 5 kap. 12 § 2 mom. i polislagen. Vid militär underrättelseinhämtning kan tillståndet utsträckas till att gälla även annan tid än tid som är betydelsefull för en viss händelse, eftersom det typiska för underrättelse kan vara inhämtande av information under en längre tid. Det väsentliga är att informationens relevans kan motiveras. Som exempel kan nämnas en sådan situation där det finns behov att utreda de teleadresser och den teleterminalutrustning som har registrerats i telesystemet via en viss basstation i närheten av ett visst område eller en viss plats samt huruvida vissa aktörer som är föremål för användningen av metoder för underrättelseinhämtning har rört sig på detta område och hur ofta.

När basstationsuppgifter inhämtas är det inte fråga om ett lika betydande ingripande i skyddet för grundläggande fri- och rättigheter som vid t.ex. teleavlyssning. Ett tillstånd som avser en viss basstation innebär inte ännu att den teleterminalutrustning eller den teleadress som är föremål för militär underrättelseinhämtning kommer att registreras på basstationen, utan situat-

ionen kan delvis också betraktas som ett slags observation av de teleterminalutrustningar och teleadresser som registreras på basstationen.

I 3 mom. föreskrivs vad som ska nämnas i ett yrkande och i ett beslut om inhämtande av basstationsuppgifter. I fråga om detta kan det i huvudsak hänvisas till det som framförs i detaljmotiveringen till 32 § 3 mom. Eftersom inhämtandet av basstationsuppgifter inte är bundet till någon specifik person utan till en tidpunkt och plats som är betydelsefull med avseende på underrättelseuppdraget, är det tillräckligt om endast de fakta som gäller underrättelseuppdraget nämns i yrkandet eller beslutet. I ett yrkande och i ett beslut bör det motiveras varför inhämtandet av basstationsuppgifter ska gälla en viss tidsperiod och vad man eftersträvar att utreda genom inhämtande av basstationsuppgifterna. I ljuset av proportionalitetsprincipen kan tidsperioden inte överskrida sex månader utom i ytterst exceptionella fall.

Momentets 3 punkt ska tillämpas så att det är fråga om sådana fakta på basis av vilka det område där basstationen finns och t.ex. vissa personer som eventuellt rör sig där kan anses vara väsentliga med avseende på underrättelseuppdraget.

**39 §.** *Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning.* Enligt 1 mom. får militärunderrättelsemyndigheten för utförande av ett underrättelseuppdrag inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning. För inhämtande av identifieringsuppgifter används en sådan teknisk anordning som militärunderrättelsemyndigheten använder. Förutsättningen för inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning är en sådan allmän förutsättning för användning av metoder för underrättelseinhämtning enligt vilken det med fog kan antas att man genom en metod för underrättelseinhämtning får information om verksamhet som avses i 4 §.

Genom befogenheten inhämtas uppgifter som identifierar en sådan teleanslutning eller teleterminalutrustning som används av personer eller som befinner sig i utrymmen eller områden som är väsentliga med avseende på underrättelseuppdraget med hjälp av en teknisk anordning som myndigheten själv använder utan att det är nödvändigt att koppla in teleoperatörer i myndigheternas inhämtande av information.

Den information som ska inhämtas gäller inte inhämtande av uppgifter om teleterminalutrustningens läge, utan genom befogenheten inhämtas information som behövs för identifiering av teleterminalutrustning, t.ex. telefonens IMEI-kod eller en IP-adress. Information inhämtas inte om var en person befinner sig vid olika tidpunkter utan om uppgifter som behövs för identifiering av den teleterminalutrustning eller teleanslutning som personen innehar eller kan tänkas använda. Den inhämtade informationen kan användas t.ex. när andra metoder för underrättelseinhämtning ska riktas in.

I 2 mom. föreskrivs om Kommunikationsverkets rätt att kontrollera den anordning som används vid inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning.

Med tekniska medel och genom övervakning ska det säkerställas att anordningen p.g.a. sina egenskaper inte medför skadliga störningar för anordningar och tjänster i det allmänna kommunikationsnätet. I praktiken kan en mindre och kortvarig störning tillåtas, men anordningen får dock inte medföra mer än ringa eller långvariga störningar. I praktiken har det observerats att en teknisk anordning som används vid inhämtandet av identifieringsuppgifter för en teleadress eller teleterminalutrustning kan orsaka tillfälliga och ringa störningar för någon annan anordning i närheten.

Vid militär underrättelseinhämtning är det inte ändamålsenligt att begränsa en i paragrafen avsedd teknisk anordning i fråga om sin funktionalitet till enbart identifiering av en teleadress och teleterminalutrustning. Detta gäller särskilt teleavlyssning och teleövervakning som genomförs vid underrättelseinhämtning som avser utländska förhållanden.

**40 §.** *Installation och avinstallation av anordningar, metoder eller programvara.* Enligt 1 mom. har en militärunderrättelsemyndighet 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 sådana föremål, ämnen, egendom, utrymmen, platser av annat slag eller informationssystem som åtgärden riktas mot, om det behövs för användningen av nämnda metod för underrättelseinhämtning. För att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran har en tjänsteman som använder metoden för underrättelseinhämtning då rätt att i hemlighet ta sig in i ovannämnda objekt och i ett ovannämnt informationssystem och att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemens säkerhetssystem. Detta medför dock inte några skyldigheter för företag att försämra datasäkerheten för sina anordningar eller produkter eller begränsningar för användningen av krypteringsteknik.

På grund av underrättelseverksamhetens karaktär får installation eller avinstallation av anordningar, metoder eller programvara inte medföra synliga olägenheter för t.ex. den allmänna datatrafiken. För varje metod för underrättelseinhämtning ska det vara fastställt vem eller vilka metoden för underrättelseinhämtning får rikta sig mot och i vilket syfte metoden får användas. På grund av detta gäller installation av anordningar, metoder eller programvara i praktiken inte i sin helhet t.ex. datasystem, där uppgifter om en på förhand icke-avgränsad användargrupp behandlas, eftersom inhämtandet av uppgifter om den aktör som är föremål för användningen av en metod för underrättelseinhämtning på detta sätt inte är ändamålsenligt eller tillåtet.

Motsvarande bestämmelse i en gällande lag finns t.ex. i 5 kap. 26 § 1 mom. i polislagen. I paragrafen finns inte särskilda krav för en tjänsteman vid Försvarsmaktens underrättelsetjänst, som får utföra de åtgärder som avses i momentet. Användning av metoder för underrättelseinhämtning kan förutsätta att en teknisk expert anlitas vid installation och avinstallation av anordningar, metoder eller programvara. Exempelvis skydd av vissa objekt eller datasystem kan förutsätta att de tillfälligt kringgås, låses upp eller passeras.

I praktiken fås tillstånd för installation och avinstallation av anordningar, metoder eller programvara i samband med ett beslut eller tillstånd som gäller användning av befogenheten.

Enligt 2 mom. får 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 installeras i utrymmen som används för stadigvarande boende endast, om domstolen har gett tillstånd till det på yrkande av Huvudstabens underrättelsechef eller på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Om en domstol beslutar om användning av en metod för underrättelseinhämtning ska det även i det tillstånd som gäller användning av en metod för underrättelseinhämtning särskilt begäras och tillåtas installation av anordningar, metoder eller programvara. Däremot behövs tillstånd inte för avinstallation av anordningar, metoder eller programvara. Om en tjänsteman vid en militärunderrättelsemyndighet beslutar om användning av en metod för underrättelseinhämt-

ning, är det motiverat att i beslutet anteckna all nödvändig information som gäller installation eller avinstallation av anordningar, metoder eller programvara.

Installation och avinstallation av anordningar, metoder eller programvara utgör en sekundär befogenhetsbestämmelse, som möjliggör användning av en egentlig metod för underrättelseinhämtning. Detta eliminerar inte skyldigheten att söka tillstånd för t.ex. användning av teleavlyssning eller teleövervakning.

En tjänsteman som är anställd hos militärunderrättelsemyndigheten har rätt att i hemlighet ta sig in i ett utrymme eller någon annan plats eller ett datasystem för att installera, ta i bruk eller avinstallera anordningar, metoder eller programvara. Även skyddet av objekt eller datasystem kan tillfälligt kringgås, låsas upp eller passeras. Skyddet kan även tillfälligt störas. Denna befogenhet möjliggör dock inte s.k. husrannsakan som anmäls i efterhand. På grund av underrättelseverksamhetens karaktär kan det bli fråga om att installation av anordningar, metoder eller programvara förutsätter intrång i skyddet av hemfriden, eftersom det t.ex. vid teknisk observation av utrustning kan vara nödvändigt att installera en anordning eller programvara på en anordning som tillhör föremålet för åtgärden i ett utrymme som används för stadigvarande boende.

I bestämmelsen tas inte ställning till hur tidigt en anordning, metod eller programvara kan installeras eller hur sent den kan avinstalleras, utan denna fråga får avgöras av tillämparen. Det är inte acceptabelt att något föremål för teknisk observation hålls utrustat för teknisk observation i all evighet. Med detta avses uttryckligen sådana anordningar som en militärunderrättelsemyndighet har installerat. I detta avseende är det för att förhindra att användningen av metoder för underrättelseinhämtning röjs dock viktigt att fasta tidsgränser inte fastställs, utan att bestämmelsen ger rörelsefrihet. Det kan hända att installation, ibruktagande eller avinstallation inte kan göras när det behövs, utan först då det blir möjligt på grund av kunskap och medvetenhet hos den person eller de personer som är föremål för åtgärden.

I samband med installation och avinstallation av anordningar, metoder eller programvara bör man alltid överväga den eventuella risk för att åka fast som detta medför samt även risken för skada hos föremålet för installationen. Exempelvis programvara som i hemlighet har installerats i ett datasystem innehåller alltid en möjlig risk för datasystemets funktion och kan försämra dess säkerhet. Militärunderrättelsemyndigheternas åtgärder får således inte föranleda större skada eller olägenhet än vad som är nödvändigt i samband med installationen eller avinstallationen av anordningen, metoden eller programvaran.

**41 §.** *Täckoperation.* I 1 mom. definieras täckoperation. Med täckoperation avses till skillnad från t.ex. observation allt sådant inhämtande av information i interaktion där exempelvis falska, vilseledande eller förtäckta uppgifter används för att förvärva förtroende hos en person eller grupp av personer eller för att hemlighålla inhämtandet av information.

Typiskt för underrättelseverksamhet är verksamhetens planenlighet och långsiktighet. Täckoperation kan innebära långvarigt umgänge, att ett förtroendeförhållande byggs upp eller infiltration i en sammanslutning som är föremål för en åtgärd. Föremål för en täckoperation kan t.ex. vara infiltration i en militär aktörs truppförband från en främmande stat.

Till skillnad från gällande befogenheter som avser utredning av brott kan en täckoperation också rikta sig mot en grupp av personer.

Föremålet för infiltrationen kan också vara en sådan grupp av personer där syftet är att inhämta information om gruppens bakomliggande verksamhet. Det kan vara fråga om en grupp av personer eller en organisation som styr eller påverkar verksamheten i den grupp av personer som är föremål för en åtgärd, t.ex. en utländsk militärunderrättelsetjänsts verksamhet som genom s.k. hybridpåverkan strävar efter att påverka Finlands nationella intressen.

Den person eller grupp av personer som är föremålet behöver inte namnges eller specificeras i fråga om t.ex. sina fysiska egenskaper, utan det räcker att personen eller gruppen av personer kan specificeras t.ex. utifrån personens eller gruppens verksamhet.

Genomförandet av täckoperationer kräver som underrättelseinhämtningsmetod omfattande resurser och långsiktig utbildning om exempelvis ett visst samhälles eller en viss sammanslutnings verksamhetssätt och praxis.

Från täckoperation ska som fristående befogenhet särskiljas skyddande av militär underrättelseinhämtning, som det föreskrivs om nedan i 72 §. Skydd av underrättelse kan dock komma på fråga i samband med täckoperation när nödvändig bakgrundsinformation skapas för en täckoperationsidentitet.

I 2 mom. föreskrivs det om situationer där militärunderrättelsemyndigheterna kan använda täckoperation. Militärunderrättelsemyndigheterna får i ett underrättelseuppdrag använda täckoperation, om det är nödvändigt att få information med avseende på uppdraget. Den förutsättning som gäller nödvändighet motsvarar förutsättningarna för användning av hemliga metoder för inhämtande av information, och bestämmelser om detta finns i 5 kap. 2 § i polislagen. I den regeringsproposition som gäller gällande polislag (RP 224/2010 rd, s. 40–43 och 94 och 95) har innebörden i begreppet ”nödvändig” närmare redogjorts för i det avsnitt i den allmänna motiveringen som gäller förutsättningarna för användning av metoder för inhämtande av information.

Utöver nödvändighet är en förutsättning för användning av täckoperation att den riktar sig mot organiserad verksamhet. Organiserad verksamhet förknippas ofta med planenlighet. Det att planenligheten nämns i bestämmelsen innebär också att det är möjligt att även i fortsättningen rikta in en metod t.ex. på en och samma enskilda aktörs planenliga verksamhet. En förutsättning för täckoperationer är att det är nödvändigt att använda dem med avseende på den kontinuitet eller upprepning som kan förutses i den verksamhet som är föremål för militärunderrättelse. Med detta avses att verksamheten inte behöver vara planenlig, organiserad eller yrkesmässig, men att den kan antas vara kontinuerlig eller den kan antas bli upprepad, varvid det kan vara fråga om t.ex. enskilda icke-organiserade personer.

Vid täckoperationer ska militärunderrättelsemyndigheterna ha en förhandsuppfattning om mot vem eller vilka eller mot vilken verksamhet täckoperationen ska riktas.

Till skillnad från den täckoperation som avses i gällande lagstiftning möjliggör den föreslagna bestämmelsen att täckoperation används också vid inhämtande av information om en grupp av personer.

Det kan också vara möjligt att rikta in infiltrationen på en sådan grupp av personer där syftet är att inhämta information om gruppens bakomliggande verksamhet. Det kan vara fråga om en grupp av personer eller en organisation som styr eller påverkar verksamheten i den grupp av personer som är föremål för en åtgärd, t.ex. en utländsk underrättelsetjänsts verksamhet som genom s.k. hybridpåverkan strävar efter att påverka Finlands nationella intressen.

De utrymmen som används för stadigvarande boende begränsar användningen av metoder för underrättelseinhämtning. Befogenhet för täckoperationer berättigar inte någon att på egen hand gå in i ett utrymme som används för stadigvarande boende. Ett undantag från denna allmänna bestämmelse finns dock i paragrafens 3 mom. Enligt momentet får den person som företar en täckoperation för att förhindra att han eller hon avslöjas gå in i en bostad under en täckmantel som skapats för ändamålet, om detta sker under aktiv medverkan av den som använder bostaden. En tjänsteman vid Försvarsmaktens underrättelsetjänst som företar täckoperationer kan ofta inte utan att avslöja sig ens vägra gå in i en bostad i en sådan situation. Med användning av en bostad avses faktisk användning. I praktiska situationer är det inte möjligt att på ett tillförlitligt sätt förvissa sig om vem som är bostadens ägare eller lagliga innehavare. Därför gäller momentet den som använder bostaden. I sådana situationer som avses i momentet kan det bli fråga om alla sådana uttryckliga och konkludenta viljeyttringar som kan tolkas så att personen i fråga har godkänt tillträdet till eller vistelsen i bostaden.

Vid täckoperationer är det dock skäl att försöka undvika att täckoperationen hamnar i ett utrymme som används som bostad. Detta kräver att täckoperationen planeras noggrant.

Enligt 4 mom. får en täckoperation även företas i ett datanät. För interaktion mellan människor i datanät är det även i övrigt typiskt att man inte alltid med säkerhet känner till den andra partens identitet. Vid täckoperationer i datanät måste det göras en bedömning av vilken typ av åtgärder som en tjänsteman vid Försvarsmaktens underrättelsetjänst ska genomföra. Täckoperationer i datanät är möjliga, om de kan antas vara av synnerlig vikt med avseende på underrättelseuppdraget.

Täckoperationer i datanät är vad genomförandet beträffar avsevärt enklare och säkrare än normala täckoperationer. Täckoperationer som företas i datanät kan bedömas vara en huvudsaklig befogenhet vad gäller täckoperationer.

Vid täckoperationer i datanät måste man beakta t.ex. sådana situationer där det för registrering i en viss tjänst krävs s.k. stark autentisering enligt lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Användning av stark autentisering kräver förberedande åtgärder som är typiska för täckoperationer och för att kunna verka i datanäten krävs sådana identifikatorer som väcker ett starkt förtroende utåt. Att enbart registrera sig i ett för alla öppet diskussionsforum under signatur och att följa med diskussionerna på forumet kan inte betraktas som en täckoperation, eftersom det som är typiskt för täckoperationer, dvs. att skapa ett förtroendeingivande förhållande och att använda falska, vilseledande eller förtäckta uppgifter, inte uppfylls i dessa fall. Enbart registrering med falska uppgifter bör betraktas som förtäckt inhämtande av information, om avsikten på exempelvis ett allmänt diskussionsforum inte är att aktivt diskutera med enskilda personer.

Vid täckoperationer i datanät ska militärunderrättelsemyndigheten ha förhandsuppgifter om t.ex. på vilka diskussionsforum en person eller en grupp av personer som är väsentlig med avseende på underrättelseuppdraget är aktiv eller vilken kommunikationskanal t.ex. en person som är väsentlig med avseende på underrättelseuppdraget använder innan det är möjligt att börja bygga upp ett sådant förtroendeingivande förhållande som täckoperationen innebär.

**42 §.** *Framställning om och plan för en täckoperation.* Enligt 1 mom. ska det i en framställning om täckoperation nämnas 1) den som föreslagit åtgärden, 2) den person eller grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information, 3) det underrättelseuppdrag 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. I den bedömning som avses i 6 punkten kan t.ex. en plan för hävande av en täckoperation beaktas.

I momentet räknas detaljerat upp den information som behövs till stöd för uppgörandet av planen och beslutsfattandet.

Enligt 2 mom. ska över en täckoperation göras upp en sådan skriftlig plan 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 ständig skyldighet att följa upp täckoperationen.

**43 §.** *Beslut om en täckoperation.* Enligt 1 mom. ska beslut om en i 41 § avsedd täckoperation fattas av Huvudstabens underrättelsechef. Beslut om en täckoperation som enbart ska genomföras i ett datanät ska fattas av en för uppdraget förordnad och med metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Det är inte nödvändigt att föreskriva om det domstolsavgörande som ska meddelas om förutsättningarna för en täckoperation. När det gäller täckoperation som används som metod för underrättelseinhämtning ska det föreligga en stark presumtion om att den information som inhämtats inte kommer att användas i en straffprocess. Fastän detta under ytterst exceptionella omständigheter är möjligt är domstolens bedömning av förutsättningarna för en täckoperation inte i motsvarande utsträckning nödvändig på samma sätt som anges i 5 kap. i polislagen och 10 kap. i tvångsmedelslagen, eftersom underrättelseombudsmannen övervakar civil underrättelseinhämtning och användningen av metoder för underrättelseinhämtning. På grund av täckoperationernas känsliga karaktär är det ändamålsenligt att besluten fattas internt av organisationen. Detta gör det lättare att hålla känslig verksamhet hemlig, eftersom information inte behöver överföras från en organisation till en annan. Dessutom försiggår militär underrättelseverksamhet även utanför Finlands gränser, och därför är en domstol inte behörig att fatta beslut i ärendet.

Nivån på beslutsfattandet motsvarar beslutsfattandet enligt 5 kap. i polislagen, och den är förenlig med förslaget till lag om civil underrättelseverksamhet. Det är inte nödvändigt att i lagen föreskriva om det domstolsavgörande som ska meddelas om förutsättningarna för en täckoperation. När det gäller täckoperation som används som metod för underrättelseinhämtning ska det föreligga en stark presumtion om att den information som inhämtats inte kommer att användas i en straffprocess. Fastän detta under ytterst exceptionella omständigheter är möjligt är domstolens bedömning av förutsättningarna för en täckoperation inte i motsvarande utsträckning nödvändig på samma sätt som anges i 5 kap. i polislagen och 10 kap. i tvångsmedelslagen, eftersom underrättelseombudsmannen övervakar militär underrättelseinhämtning och användningen av metoder för underrättelseinhämtning.

Beslut enligt 2 mom. om en täckoperation får meddelas för högst sex månader åt gången.

Enligt 3 mom. i paragrafen ska beslut om en täckoperation fattas skriftligen. I beslutet ska följande nämnas: 1) den som föreslagit åtgärden, 2) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som ansvarar för genomförandet av täckoperationen, 3) identifikationsuppgifterna för de tjänstemän som genomför täckoperationen, 4) det underrättelseuppdrag som ligger till grund för åtgärden, 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) beslutets giltighetstid, 9) eventuella begränsningar i

och villkor för täckoperationen. Bestämmelsen motsvarar i huvudsak 5 kap. 32 § 3 mom. i den gällande polislagen.

Med de identifikationsuppgifter som avses i 3 mom. 3 punkten avses sådan information som kan identifiera den tjänsteman som genomför täckoperationen under och efter täckoperationen.

I paragrafens 4 mom. föreskrivs att beslutet vid behov ska ses över när omständigheterna förändras. Beslut om avslutande av en täckoperation ska fattas skriftligen.

**44 §**. *Brottsförbud.* I 1 mom. konstateras för tydlighetens skull att en tjänsteman vid en militärunderrättelsemyndighet som företar en täckoperation inte får begå brott eller ta initiativ till ett brott. Även sådana initiativ som inte ännu är anstiftan till brott enligt strafflagen är förbjudna för den som företar en täckoperation.

I 2 mom. föreskrivs om vissa situationer när ansvarsfrihet gäller vid brott. Om en tjänsteman vid en militärunderrättelsemyndighet som företar en täckoperation begår en trafikförseelse, en ordningsförseelse eller något annat jämförbart brott för vilket det föreskrivna straffet är ordningsbot, går tjänstemannen fri från straffansvar, om gärningen har varit nödvändig för att syftet med täckoperationen ska nås eller för att inhämtandet av information inte ska avslöjas.

Bestämmelsen är inte generell i det avseende att en tjänsteman vid en militärunderrättelsemyndighet som företar en täckoperation automatiskt kan befrias från straffansvar om han eller hon begår ett sådant brott som avses i paragrafen. I lagen finns många bestämmelser utifrån vilka en tjänsteman har rätt att handla på ett visst sätt, som utan en uttrycklig bestämmelse om befogenhet skulle betraktas som lagstridigt förfarande. Enligt 48 § 5 mom. i vägtrafiklagen (267/1981) 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 i observationsuppgifter och vid tekniska observationsuppgifter och en polisman i täckoperationsuppgifter och uppgifter som har samband med bevisprovokation genom köp 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.

Ansvarsfrihet kan komma på fråga endast när det konstateras att gärningen har varit nödvändig för att syftet med täckoperationen ska nås eller för att inhämtandet av information inte ska avslöjas. Befrielse från straffansvar gäller således i rätt begränsad utsträckning. I förhållande till nämnda 48 § 5 mom. i vägtrafiklagen ska den föreslagna bestämmelsen tillämpas t.ex. när en tjänsteman som företar en täckoperation inte har iakttagit särskild försiktighet. I sådana fall tillämpas inte det nämnda momentet. En tjänsteman som företar en täckoperation kan i detta fall befrias från straffansvar på basis av det föreslagna momentet.

Först bedöms militärunderrättelsemyndighetens tjänstemans förfarande av underrättelseombudsmannen, som övervakar underrättelseverksamheten.

**45 §.** *Bevisprovokation genom köp.* Enligt 1 mom. avses med bevisprovokation genom köp ett köpeanbud eller köp av ett föremål, ett ämne, egendom eller en tjänst som en militärunderrättelsemyndighet gör i syfte att ta om hand eller hitta ett föremål, ett ämne, egendom eller information som har samband med ett underrättelseuppdrag.

Bevisprovokation genom köp kan komma på fråga t.ex. när det gäller sådant material som används för framställning av falska handlingar och som underrättelsetjänsten i en främmande

stat kan tänkas använda. Det kan också vara fråga om programvara som eventuellt används för att skada samhällets vitala funktioner eller framställning av sådan programvara som kan användas för allvarliga cyberattacker som är riktade mot samhällets vitala funktioner. Militärunderrättelsemyndigheterna kan i detta fall inhämta information om en aktör genom att lägga fram ett köpeanbud om framställning av sådan programvara eller skaffa ett prov på programvara av detta slag.

Avsikten är också att inhämta information om aktörer som är i kontakt med en viss säljare. Genom bevisprovokation genom köp kommer man nära den säljare som kopplas till ett visst underrättelseuppdrag, och på detta sätt kan man också inhämta information om vem som skaffar tjänster och utrustning av en viss säljare.

Bestämmelser om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten finns i 46 § 1 mom. för att beslutsfattandet i detta fall avviker från huvudregeln. Bevisprovokation genom köp måste dock särskiljas från underrättelseinhämtning på basis av en allmänt tillgänglig annons.

I samband med bevisprovokation genom köp är det möjligt att även vidta förberedande åtgärder, t.ex. lagring eller flyttning av det gods som är föremål för bevisprovokationen genom köp före det egentliga köpeanbudet eller köpet, och i detta fall kan åtgärden även utgöra en del av vederlaget.

I 2 mom. föreskrivs det om förutsättningarna för bevisprovokation genom köp. Militärunderrättelsemyndigheterna får genomföra bevisprovokation genom köp, om det är nödvändigt för att få information med avseende på ett underrättelseuppdrag.

Enligt 3 mom. får den som genomför bevisprovokation genom köp utföra bara sådant inhämtande av information som är nödvändigt för genomförandet av 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 denne inte annars skulle begå.

Bevisprovokation genom köp är ofta omöjligt att genomföra, om den inte föregås av en fas med informationsinhämtning och handelsförhandlingar samt en naturlig fas med frigörande från köpslutet. Före bevisprovokationen genom köp måste man kunna försäkra sig om att det föremål, det ämne, den egendom eller den tjänst som är föremål för bevisprovokationen genom köp innehas av den person som är föremål för åtgärden, varvid det är möjligt att utesluta risken för brottsprovokation. På grund av dessa omständigheter konstateras det uttryckligen i momentet att den som genomför bevisprovokation genom köp får utföra bara sådant inhämtande av information som är nödvändigt för genomförandet av bevisprovokationen. Med en befogenhet som gäller bevisprovokation genom köp får man inte kringgå t.ex. befogenheten för täckoperation genom att endast inhämta information utan att eftersträva egentlig bevisprovokation genom köp.

I momentet nämns uttryckligen att 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 denne inte annars skulle begå. Om det för en bevisprovokation genom köp är nödvändigt att anlita någon utomstående person för att exempelvis etablera kontakt mellan den person som genomför bevisprovokationen och den person som är föremål för den, måste man försäkra sig om att bevisprovokationen inte leder till att den utomstående personen begår ett brott när han eller hon etablerar kontakt. Däremot kan militärunderrättelsemyndighetens utredningsskyldighet inte vara särdeles sträng, eftersom utomstående personers verksamhet i förhållande till bevis-

provokationen genom köp ofta ligger utanför militärunderrättelsemyndigheternas påverkningsmöjligheter. Det förbud som det är fråga om gäller naturligtvis framför allt den person som köpeanbudet riktas till eller som man köper av.

I paragrafens 4 mom. nämns det 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. Den reglering som nu är aktuell är motiverad av rättsskyddsskäl, eftersom bevisprovokationen genom köp också kan genomföras i en bostad. Det är motiverat att bestämmelserna är i linje med ett motsvarande krav som gäller täckoperation.

**46 §.** *Beslut om bevisprovokation genom köp.* Enligt det föreslagna 1 mom. ska Huvudstabens underrättelsechef fatta beslut om bevisprovokation genom köp. Beslut om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten får fattas också av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Vid bevisprovokation genom köp som gäller säljanbud till allmänheten är risken för brottsprovokation i princip liten, och då kan också beslutsnivån vara lägre.

Enligt det föreslagna 2 mom. ska beslut om bevisprovokation genom köp få meddelas för högst sex månader åt gången.

Enligt det föreslagna 3 mom. ska beslut om bevisprovokation genom köp fattas skriftligen. I beslutet ska nämnas 1) det underrättelseuppdrag som ligger till grund för åtgärden, 2) den person som är föremål för bevisprovokationen, 3) de fakta som förutsättningarna för och inriktningen av bevisprovokationen genom köp 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 med användningen av metoder för underrättelseinhämtning särskilt förtrogna militärjurist eller tjänsteman som leder och övervakar bevisprovokationen genom köp, och 8) eventuella begränsningar och villkor för bevisprovokationen.

Den resultatförväntan (3 punkten) som är förknippad med en bevisprovokation genom köp har samband med kravet på sannolikhet. Enligt 45 § ska en bevisprovokation genom köp vara nödvändig för att få information med tanke på ett underrättelseuppdrag.

Bevisprovokation genom köp kan också rikta sig mot en person som handlar så att säga i god tro. Bevisprovokation genom köp kan liksom för närvarande rikta sig också mot någon annan än en försäljare. Så förutsätter t.ex. en effektiv underrättelseinhämtning om en främmande stats militära underrättelsetjänsts verksamhet att militärunderrättelsemyndigheterna får tillräckligt med information om den främmande statens militära underrättelsetjänsts verksamhet, betalningsförbindelser och om den bakomliggande organisationen och dess ledning. I en sådan situation kan bevisprovokationen genom köp behöva riktas t.ex. mot en handelspartner till den aktör som beskrivs ovan.

**47 §.** *Plan för genomförande av bevisprovokation genom köp.* Enligt 1 mom. ska det upprättas en skriftlig plan över genomförandet av bevisprovokation genom köp, om detta behövs med hänsyn till operationens omfattning eller andra motsvarande skäl. Enligt 2 mom. ska planen för genomförande av bevisprovokationen vid behov ses över vid förändrade omständigheter.

Paragrafen motsvarar 5 kap. 37 § i polislagen. En separat plan för genomförande av bevisprovokation genom köp kan behövas särskilt för att avvärja de risker som är förknippade med verksamheten.

Till följd av att bevisprovokation genom köp är krävande och både bevisprovokationen och underrättelseverksamheten är förknippade med risker behöver en plan i praktiken upprättas vid alla operationer. En plan behöver inte upprättas om bevisprovokationen genom köp görs t.ex. utifrån en enkel tidningsannons eller någon annan motsvarande orsak.

Skyldigheten att se över planen innebär en ständig skyldighet att följa upp bevisprovokationen genom köp. Det finns inga hinder för att också upprätta en plan för att avveckla bevisprovokation genom köp, om upprättandet av en sådan plan är möjligt och behövligt när bevisprovokationen planeras.

**48 §.** *Beslut om genomförande av bevisprovokation genom köp.* Enligt 1 mom. ska beslut om genomförande av bevisprovokation genom köp fattas skriftligen. Beslutet ska fattas av en sådan för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller en annan tjänsteman som ansvarar för genomförandet av bevisprovokation genom köp. Användningen av bevisprovokation genom köp sker alltså i två moment. Det praktiska genomförandet av bevisprovokation genom köp kräver först ett beslut om bevisprovokation genom köp, varefter det ska fattas ett separat beslut om genomförande av bevisprovokation genom köp när det finns tillfälle att genomföra bevisprovokationen.

Enligt det föreslagna 2 mom. ska i beslutet nämnas 1) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som beslutat om bevisprovokationen, 2) identifikationsuppgifter för de tjänstemän vid militärunderrättelsemyndigheterna 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, och 4) eventuella begränsningar och villkor för bevisprovokationen.

I 3 mom. föreskrivs det att om åtgärden inte tål uppskov, behöver ett beslut som avses i 2 mom. inte upprättas i skriftlig form före bevisprovokationen inleds. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter bevisprovokationen.

Enligt 4 mom. ska beslutet om genomförande av bevisprovokationen vid behov ses över vid förändrade omständigheter.

Syftet med en mångdubbel dokumentprocess är att säkerställa att en bevisprovokation genom köp kan genomföras på behörigt sätt. Dessutom blir hela processen tillförlitligt dokumenterad, om det uppstår behov av eftersyn. I synnerhet med tanke på de risker som är förknippade med genomförande av bevisprovokation genom köp är det möjligt att verksamheten behöver ses över även i efterhand.

**49 §.** *Användning av informationskällor.* I det föreslagna 1 mom. finns en definition av begreppet användning av informationskällor. Med användning av informationskällor avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för den militära underrättelseinhämtningen och kontakt med personer som inte hör till en finsk myndighet (*informationskälla*). Användningen av informationskällor är en av de viktigaste metoderna för inhämtande av information när det gäller personbaserad underrättelseinhämtning.

Som sådana informationskällor som avses i definitionen anses varken enskilda uppgiftslämnare eller tjänstemän. Det ska inte anses vara styrd användning av en informationskälla när informationskällan på eget initiativ berättar för militärunderrättelsemyndigheterna om omständigheter som antas intressera dessa och som myndigheterna utnyttjar enligt egen prövning.

Styrd användning utmärks av att de uppgifter som informationskällan ger inhämtas utan att föremålet för underrättelseuppdraget vet om det.

Användningen av informationskällor ska särskiljas från situationer där en person annars bistår den militära underrättelseinhämtningen. En person kan bistå t.ex. genom att upplåta ett utrymme för militärunderrättelsemyndigheten under den tid en metod för underrättelseinhämtning används eller genom att ge Försvarsmaktens underrättelsetjänst rätten att vid ett underrättelseuppdrag använda identiteten av ett företag som personen grundat. Sådan verksamhet kan inte anses som användning av informationskällor. Eftersom det bistånd en person ger den militära underrättelseinhämtningen grundar sig t.ex. på den frihet personen har att använda sin egendom på det sätt denne önskar, krävs det ingen separat reglering om sådan verksamhet. Personen ska alltså frivilligt samtycka till att militärunderrättelsemyndigheten använder t.ex. egendom som personen har besittningsrätt till. En tjänsteman vid militärunderrättelsemyndigheten kan lyfta fram möjligheten att bistå av den militära underrättelseinhämtningen, men personen ska själv dra slutsatsen om att vilja bistå. Militärunderrättelsemyndigheten ska i sådana fall redogöra för att det inte finns någon lagstadgad skyldighet att bistå, utan att biståndet helt bygger på personens egen frivillighet.

Utgångspunkten vid användningen av metoder för underrättelseinhämtning är att de inte får riktas mot utrymmen som används för stadigvarande boende. Användningen av informationskällor skiljer sig emellertid från övriga befogenheter för underrättelseinhämtning genom att ingen tjänsteman genomför informationsinhämtningen. Således är informationskällans verksamhet inte inom militärunderrättelsemyndighetens kontroll, förutom i samband med styrd användning av informationskällan. När en informationskälla ombes inhämta information ska det beaktas att informationsinhämtningen inte får förutsätta tillträde till utrymmen som används för stadigvarande boende. Av denna anledning ska den tjänsteman vid militärunderrättelsemyndigheten som sköter kontakten med informationskällan underrätta informationskällan om den begränsning som avses ovan. Informationskällan får dock på samma sätt som vid en täckoperation gå in i utrymmen som används för stadigvarande boende när det behövs för att förhindra att användningen av informationskällor avslöjas.

I det föreslagna 2 mom. föreskrivs det om förutsättningarna för styrd användning av en informationskälla. Enligt momentet får militärunderrättelsemyndigheten be att en för ändamålet godkänd informationskälla som har lämpliga personliga egenskaper, har registrerats och har samtyckt till informationsinhämtning, inhämtar den information som avses i 1 mom.

Det samtycke som avses i momentet ska alltid vara genuint frivilligt. Förhållandet mellan tjänstemannen vid militärunderrättelsemyndigheten och informationskällan får inte bli osakligt t.ex. så att tjänstemannen försöker övertala informationskällan att inhämta information genom att utlova fördelar som inte kan ges med stöd av gällande lagstiftning. Ett osakligt beroendeförhållande kan också uppstå när en informationskälla blir en så viktig metod för inhämtande av information för militärunderrättelsemyndigheten att den åsidosätter andra metoder.

Orsaken till omnämnandet av att informationskällan ska ha lämpliga personliga egenskaper har att göra med att informationskällan kan ha osakliga motiv till att agera som informationskälla. Till dem hör t.ex. att sträva efter ekonomisk vinning eller någon annan fördel och hämnd. När en styrd användning av en informationskälla inleds ska det också utredas i vilket syfte och varför informationskällan går med i den styrda användningen.

I det föreslagna 3 mom. föreskrivs om de begränsningar som är förknippade med styrd användning av informationskällor och om hur inhämtande av information ska genomföras i öv-

rigt. Vid styrd användning av informationskällor ska en informationskälla inte få 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 informationskällan 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.

Andra personer än tjänstemän får inte använda sig av myndighetsbefogenheter om det inte föreskrivs uttryckligen om saken. Det föreslås inte att informationskällor ges rättigheter att använda befogenheter som riktar sig mot kärnområdet för de grundläggande fri- och rättigheterna. Även med tanke på denna utgångspunkt är det klart att en informationskälla inte får användas för att kringgå begränsningar som gäller användningen av befogenheter som tilldelats myndigheterna. Det ska t.ex. inte vara tillåtet att kringgå de begränsningar som är förknippade med stadigvarande boende genom att använda en informationskälla. Detsamma gäller t.ex. för teknisk avlyssning och optisk observation. Försvarsmaktens underrättelsetjänst ska inte kunna förse en informationskälla med tekniska anordningar som möjliggör avlyssning eller observation. Momentet följer Europadomstolens avgörandepraxis (exempelvis Allan mot Förenade kungariket).

Det ska emellertid anses vara fråga om tillåten användning av en informationskälla när informationskällan på grund av sina kontakter rör sig bland föremål för militär underrättelseinhämtning eller träffar personer som källan känner sedan tidigare samt samtalar med dem. Det ska också vara fråga om tillåtet inhämtande av information bl.a. när kontakt etableras mellan en tjänsteman vid Försvarsmaktens underrättelsetjänst, som agerar förtäckt, och den organisation som är föremål för underrättelseuppdraget. En informationskälla ska också kunna förmedla information och i begränsad omfattning fungera som t.ex. tolk. Denna verksamhetsmöjlighet begränsas dock av att den verksamhet som bedrivs av en tjänsteman vid Försvarsmaktens underrättelsetjänst eller av en informationskälla inte får leda till att källan genom sin verksamhet gör sig skyldig till brott. Undvikandet av brottsprovokation hänger samman med att militärunderrättelsemyndigheten vid användning av mellanhänder i princip ska vara passiv så att en sådan person i samband med användningen av informationskällor inte gör sig skyldig till brott (Europadomstolens avgöranden, t.ex. Vanyan mot Ryssland och Ramanauskas mot Litauen).

Militärunderrättelsemyndigheten ska inte få ge en informationskälla ett uppdrag som äventyrar informationskällans liv eller hälsa. Också informationskällans närstående kan vara utsatta för risk, vilket måste beaktas när användningen av informationskällor ordnas. Det beror på fallet om man måste trygga informationskällans säkerhet under och efter inhämtandet av information och i vilken utsträckning. Bestämmelser om särskilt tryggande av informationskällor finns nedan. Om det finns anledning att misstänka att informationskällans säkerhet behöver tryggas redan före inhämtandet av information eller om informationskällan behöver tryggas mer intensivt, blir 75 §, som gäller tryggande av informationskällor, tillämplig.

**50 §.** *Betalning av arvode till informationskällan.* Enligt den föreslagna paragrafen ska arvode kunna betalas till en registrerad informationskälla. Av grundad anledning kan arvode betalas även till en oregistrerad informationskälla. I momentet konstateras även att det i denna regeringsproposition föreslås särskilda bestämmelser om skatteplikt för arvodet.

**51 §.** *Beslut om styrd användning av informationskällor.* Enligt det föreslagna 1 mom. ska beslut om styrd användning av informationskällor fattas av Huvudstabens underrättelsechef. Be-

slutsnivån motsvarar beslutsnivån för användning av informationskällor vid utredning av brott.

Enligt det föreslagna 2 mom. får ett beslut om styrd användning av informationskällor meddelas för högst sex månader åt gången.

I det föreslagna 3 mom. föreskrivs det om vad som ska nämnas i ett beslut om styrd användning av informationskällor och skyddandet av den styrda användningen. Enligt momentet ska beslutet fattas skriftligen. I beslutet ska nämnas 1) den som föreslagit åtgärden, 2) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som ansvarar för genomförandet av underrättelseuppdraget, 3) identifikationsuppgifterna för informationskällan, 4) de faktorer som ligger till grund för åtgärden, 5) syftet med inhämtandet av information eller skyddandet och planen för genomförandet av detta, 6) beslutets giltighetstid, och 7) eventuella begränsningar och villkor för den styrda användningen av informationskällor och för skyddandet av den styrda användningen.

Enligt det föreslagna 4 mom. ska beslutet vid behov ses över när omständigheterna förändras. Beslut om att styrd användning och skyddande av informationskällor ska avslutas ska fattas skriftligen.

**52 §.** *Platsspecifik underrättelseinhämtning.* I paragrafen föreslås en definition av platsspecifik underrättelseinhämtning. Med platsspecifik underrättelseinhämtning avses underrättelseinhämtning för att hitta föremål, egendom, handlingar eller information eller utröna omständigheter i något annat utrymme än ett utrymme som används för stadigvarande boende eller ett utrymme beträffande vilket 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.

Befogenheten är ny jämfört med de hemliga metoder för inhämtande av information som avses i 5 kap. i polislagen. Platsspecifik underrättelseinhämtning genomförs i regel i hemlighet så att platsens ägare, innehavare eller någon annan person inte känner till att militärunderrättelsemyndigheten besöker platsen. Detta framgår även indirekt av namnet på metoden för underrättelseinhämtning, alltså platsspecifik underrättelseinhämtning.

Den platsspecifika underrättelseinhämtningen riktas i enlighet med definitionen mot platser eller utrymmen. Den kan för det första riktas mot platser som avses i 8 kap. 1 § 4 mom. i tvångsmedelslagen. Enligt det momentet avses med platsgenomsökning genomsökning av andra platser än sådana som avses i 2 eller 3 mom. i nämnda paragraf trots att de inte är allmänt tillgängliga eller den allmänna tillgängligheten har begränsats eller hindrats vid tidpunkten för genomsökningen, eller genomsökning av ett fordon.

Platsspecifik underrättelseinhämtning kan för det andra riktas mot sådana hemfridsskyddade platser som avses i 24 kap. 11 § i strafflagen, dock inte mot utrymmen som används för stadigvarande boende. Föremål för platsspecifik underrättelseinhämtning kan således vara fritidsbostäder och övriga 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. Om det emellertid framgår att en plats eller ett utrymme används för stadigvarande boende, får platsspecifik underrättelseinhämtning inte förrättas där.

Platsspecifik underrättelseinhämtning får emellertid inte företas i en i 24 kap. 11 § i strafflagen avsedd hemfridsskyddad bostad, om det inte kan visas att den inte i själva verket används för något annat ändamål än för boende av permanent natur (GrUU 36/1998 rd, KKO 2009:54).

Platsspecifik underrättelseinhämtning får inte heller företas i ett utrymme beträffande vilket det finns anledning att anta att den platsspecifika 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. Sådana platser som avses i bestämmelsen är t.ex. läkarmottagningar, advokatbyråer, juridiska byråer, mediehus och tidningsredaktioner, utrymmen som används av en präst i ett sådant registrerat religionssamfund som avses i religionsfrihetslagen (453/2003) och serverhallar som kan antas förmedla i paragrafen avsedd information som omfattas av tystnadsplikt eller tystnadsrätt.

Att ovan avsedda utrymmen har en accentuerad koppling till tystnadsplikt eller tystnadsrätt konstateras med uttrycket ”ett utrymme beträffande vilket det finns anledning att anta att underrättelseinhämtningen kommer att omfatta information”. Detta uttryck betyder att platsspecifik underrättelseinhämtning inte kategoriskt, utifrån det ändamål för vilket platsen i fråga i allmänhet eller huvudsakligen används, ska omfattas av de förbud som gäller för informationsinhämtning på en plats. Platsspecifik underrättelseinhämtning kan eventuellt omfatta t.ex. en advokats bostad, om advokaten arbetar där eller om där annars finns handlingar som hänför sig till hans eller hennes arbete. Platsspecifik underrättelseinhämtning som riktas mot en advokatbyrå kan emellertid avgränsas så att den inte omfattar information som är sekretessbelagd. Eftersom avsikten till denna del är att skydda tystnadsplikten eller tystnadsrätten och inte vissa utrymmen, blir definitionen av utrymmen som berörs av platsspecifik underrättelseinhämtning nödvändigtvis i någon mån öppen och bestäms i enskilda fall i samband med noggrann prövning när beslutet om platsspecifik underrättelseinhämtning bereds.

Om den ursprungliga bedömningen av utrymmenas natur visar sig vara felaktig, ska grunderna för den platsspecifika underrättelseinhämtningen omvärderas och underrättelseinhämtningen avbrytas omedelbart.

Den platsspecifika underrättelseinhämtningens godtagbarhet med tanke på de grundläggande fri- och rättigheterna bedöms närmare i det avsnitt som handlar om lagstiftningsordningen.

Föremål för platsspecifik underrättelseinhämtning kan t.ex. vara ett stängt fordon (såsom en bil) som inte används för boende. Ett typexempel på platsspecifik underrättelseinhämtning är genomsökning av en bils bagageutrymme eller handskfack i hemlighet i syfte att hitta och kopiera ett föremål eller en handling. Andra exempel på platser som omfattas av platsspecifik underrättelseinhämtning är hotellrum, tält, husvagnar och fartyg som kan bebos samt trappuppgångar i bostadshus, butiker, ämbetsverk, kaféer och rum i affärslokaler.

För att komma in i ett stängt utrymme kan det i vissa fall krävas att ett hinder avlägsnas, t.ex. att en låst dörr eller skåpdörr måste öppnas på ett sätt som är lämpligt med tanke på omständigheterna.

Inom underrättelseinhämtning behövs det ibland flera mellanhänder för att förmedla informationen, och det kan finnas behov av att utreda vem som vidareförmedlar informationen. Inom underrättelseverksamheten är det rätt vanligt att använda t.ex. gömställen och postlådor för att kunna gömma information på olika platser. Försändelsens avsändare och mottagare träffas inte och risken för att bli avslöjad minskar. För den militära underrättelseinhämtningen är det mycket viktigt att i hemlighet kunna rikta informationsinhämtning mot sådana platser som

nämns ovan och att kunna kopiera t.ex. utländska militära organisationers interna och externa kommunikation.

Den hänvisning till plats som görs i paragrafen är ett överordnat begrepp som omfattar utrymmen och andra platser. De sistnämnda avser närmast utomhusområden. Med hänvisningen till utrymme avses platser som avgränsats av väggar och vanligen också av tak.

Syftet med platsspecifik underrättelseinhämtning är att finna information som är betydelsefull med tanke på föremålen för militär underrättelseinhämtning. Vid platsspecifik underrättelseinhämtning är det dock inte tillåtet att omhänderta föremål, dokument eller annan egendom som finns i utrymmet, utan nödvändig information om dem ska lagras t.ex. 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 förutsätter att föremålet tas om hand.

När det fattas beslut om platsspecifik underrättelseinhämtning ska det särskilt tas fasta på att de grundläggande och mänskliga rättigheterna tillgodoses, i synnerhet när man överväger att rikta den platsspecifika underrättelseinhämtningen mot ett hemfridsskyddat område.

Bestämmelser om underrättelse om platsspecifik underrättelseinhämtning till den som varit föremål för den samt till platsens ägare eller innehavare finns i 86 §.

**53 §.** *Beslut om platsspecifik underrättelseinhämtning.* I paragrafen föreslås bestämmelser om beslut om platsspecifik underrättelseinhämtning.

Enligt det föreslagna 1 mom. ska beslut om platsspecifik underrättelseinhämtning fattas av domstol, när den riktas mot en hemfridsskyddad plats eller mot en plats som allmänheten inte har tillträde till eller dit det tillträdet för allmänheten har begränsats eller förhindrats. Av befogenhetens natur följer att militärunderrättelsemyndigheten med stöd av domstolens beslut har rätt att gå in i ett stängt utrymme genom att passera låset till en dörr eller något annat hinder som hindrar tillträde eller på något annat sätt som med hänsyn till omständigheterna kan anses ändamålsenligt.

Även om man genom platsspecifik underrättelseinhämtning inte riktar sig mot kärnområdet för de grundläggande fri- och rättigheterna, är det motiverat att ge domstolen befogenheten att fatta beslut i de fall som avses i 1 mom. med hänsyn till att den platsspecifika underrättelseinhämtningen är en verksamhet som avses ske obemärkt. Detta beror på att man vid platsspecifik underrättelseinhämtning inte tillämpar samma förfarande som vid husrannsakan. Föremålet för informationsinhämtningen har då inga möjligheter att kontrollera myndighetens verksamhet på samma sätt som vid allmän husrannsakan eller platsgenomsökning.

I det föreslagna 2 mom. föreskrivs det att om det ärende som avses i 1 mom. inte tål uppskov, får Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman besluta om platsspecifik underrättelseinhämtning till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast inom 24 timmar från det att metoden började användas.

Beslutsfattande i brådskande fall är i praktiken mycket sällsynt, eftersom avsikten är att Helsingfors tingsrätt ska ha jour dygnet runt.

Om domstolen i fråga om ett beslut som fattats i en brådskande situation anser att det inte funnits förutsättningar för åtgärden, ska användningen av metoden för underrättelseinhämtning avslutas och det material och de anteckningar om informationen som fåtts på detta sätt omedelbart utplånas. Bestämmelser om skyldigheten att förstöra material i dessa fall finns nedan i 84 §.

Enligt 3 mom. ska beslut om annan platsspecifik underrättelseinhämtning än den som avses i 1 mom. fattas av Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Momentet omfattar sådana platser som är allmänt tillgängliga och till vilka den allmänna tillgängligheten inte har begränsats eller förhindrats under den tid den platsspecifika underrättelseinhämtningen genomförs. Detsamma gäller för platsspecifik underrättelseinhämtning som riktas mot ett fordon.

Enligt 4 mom. kan tillstånd ges och beslut fattas för högst en månad åt gången.

Platsspecifik underrättelseinhämtning är en metod för underrättelseinhämtning som har som syfte att finna sådan information som kan antas vara av synnerligen stor betydelse med tanke på ett underrättelseuppdrag. Till underrättelseinhämtningens natur hör att det finns behov av att besöka en viss plats mer än en gång. Sådana situationer motiverar en längre tillståndstid. Som ett exempel kan nämnas en situation där man i samband med en platsspecifik underrättelseinhämtning behöver kopiera handlingar som är betydelsefulla med tanke på underrättelseuppdraget mer än en gång.

Enligt det föreslagna 5 mom. ska i ett yrkande och i ett beslut om platsspecifik underrättelseinhämtning tillräckligt noggrant specificeras 1) det underrättelseuppdrag som ligger till grund för åtgärden, 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, och 5) eventuella begränsningar i den platsspecifika underrättelseinhämtningen.

Enligt det föreslagna 6 mom. ska, när sakens brådskande natur kräver det, ett beslut om platsspecifik underrättelseinhämtning få dokumenteras efter att den platsspecifika underrättelseinhämtningen har genomförts.

**54 §.** *Kopiering.* Enligt paragrafen ska militärunderrättelsemyndigheterna i samband med militär underrättelseinhämtning ha rätt att kopiera ett dokument eller föremål för utförande av ett underrättelseuppdrag.

Dokumentet eller föremålet ska i regel kopieras utan omhändertagande med tanke på risken för att underrättelseinsatsen avslöjas.

Ett dokument kan i praktiken kopieras genom att man fotograferar eller skannar dokumentet t.ex. med hjälp av ett skanningsprogram i telefonen. Med kopiering av ett föremål avses t.ex. en situation där ett föremål behöver kopieras med användande av en 3D-skanner.

Kopieringen gäller fysiska dokument och föremål som existerar i verkligheten. När informationen finns i ett dokument som finns sparat i en teknisk anordning, ska uppgifterna i regel in-

hämtas med hjälp av teknisk observation av utrustning. Det är ändå tillåtet att göra anteckningar från en dators öppna bildskärm med stöd av kopieringsbefogenheten. Om de uppgifter som syns på skärmen kopieras med användande av en teknisk anordning, såsom med en kamera, är det fråga om teknisk observation av utrustning. Det är fråga om kopiering t.ex. när en nyckel kopieras för att befogenheten till platsspecifik underrättelseinhämtning ska kunna utövas, och då behöver man t.ex. inte bryta upp låset för att få tillträde till det utrymme som är föremål för platsspecifik underrättelseinhämtning.

I det föreslagna 2 mom. föreskrivs det om en specialsituation vid utövande av kopieringsbefogenheten, nämligen när kopieringen riktas mot någon annans än en statlig aktörs meddelande. Då är en särskild förutsättning för användningen av befogenheten att detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag. Förutsättningen motsvarar andra befogenheter som ingriper i skyddet för förtroliga meddelanden.

**55 §.** *Kopiering av försändelser.* Enligt paragrafen ska ett brev eller en annan motsvarande försändelse få kopieras innan den anländer till mottagaren, om kopieringen kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag och informationen hänför sig till sådan verksamhet som allvarligt hotar försvaret eller den nationella säkerheten. I fråga om brev ska det beaktas att brev omfattas av sekretessen i fråga om förtroliga meddelanden.

Paragrafen motsvarar 7 kap. 5 § i tvångsmedelslagen. Skillnaden är att man vid kopiering av försändelser inte behöver meddela försändelsens mottagare, eftersom det är fråga om en åtgärd som utförs utan att mottagaren vet om det.

I det föreslagna 2 mom. föreskrivs det om kopiering av en försändelse i en specialsituation, nämligen när kopieringen riktas mot någon annans än en statlig aktörs meddelande. Då är en särskild förutsättning för användningen av befogenheten att detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

**56 §.** *Kvarhållande av försändelser för kopiering.* I det föreslagna 1 mom. föreskrivs det att om det finns skäl att anta att ett brev eller någon annan försändelse, som får kopieras, 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 och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman förordna att försändelsen ska hållas kvar på verksamhetsstället i fråga, tills kopiering hinner utföras.

Regleringen i momentet grundar sig i huvudsak på bestämmelserna i 7 kap. 6 § 1 mom. i tvångsmedelslagen. När det gäller godstrafik är en förutsättning att det finns ett fast verksamhetsställe där försändelsen kan avhämtas eller som sörjer för att den levereras till mottagaren. Ett sådant verksamhetsställe kan t.ex. vara ett kontor där det bedrivs företagsverksamhet inom logistikområdet, om man därifrån sköter ärenden som gäller ankommande fraktgods och håller kontakt med dess mottagare.

Enligt det föreslagna 2 mom. ska ett i 1 mom. avsett förordnande få meddelas för högst en månad räknat från det att chefen för postkontoret, järnvägsstationen eller 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.

Ett förordnande får inte meddelas för längre tid än en månad, eftersom det för verksamhetsställets personal innebär en extra skyldighet att övervaka de ankommande försändelserna. Emellertid kan ett nytt förordnande meddelas när fristen för det förra förordnandet gått ut.

Enligt det föreslagna 3 mom. ska chefen för postkontoret, järnvägsstationen eller verksamhetsstället genast underrätta den som har meddelat förordnandet om när försändelsen har anlänt. Denne ska utan ogrundat dröjsmål besluta om kopiering.

Om en ankommande försändelse inte har kunnat specificeras tillräckligt noggrant och den som har meddelat förordnandet eller den som han eller hon har utsett när de anländer till verksamhetsstället genast märker, t.ex. utifrån avsändarens namn eller handstil att det är klart att det inte kan vara fråga om den försändelse som ska kopieras, får den inte öppnas eller undersökas, utan ska omedelbart vidarebefordras.

**57 §.** *Beslut om kopiering.* Enligt det föreslagna 1 mom. ska beslut om kopiering fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Utbildningskravet på tjänstemännen i fråga beror på att det är särskilt viktigt att känna till gränsen mellan kopiering och andra metoder för underrättelseinhämtning, såsom teknisk observation av utrustning. Dessa hänför sig i hög grad till hanteringen av förbud mot kopiering. Med hjälp av utbildning kan man även minska risken för att inhämtandet av information avslöjas samt främja verksamhetens resultat.

I 2 mom. föreslås bestämmelser om beslutsförfarandet i brådskande situationer. I ett enskilt fall ska också någon annan än en militärjurist eller annan tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning självständigt få fatta beslut om kopiering. Ärendet ska dock inom 24 timmar ges till den militärjurist eller andra tjänsteman som avses i 1 mom. för avgörande.

**58 §.** *Radiosignalspaning.* I det föreslagna 1 mom. föreskrivs det om radiosignalspaning med hjälp av vilken militärunderrättelsemyndigheten kan rikta informationsinhämtning mot radiofrekventa elektromagnetiska vågor, alltså radiovågor. Radiosignalspaning ska i stor omfattning kunna riktas mot kommunikation som används av olika militära objekt och mot styrningstrafik i fråga om olika tekniska anordningar.

Av delområdena inom signalspaning omfattar radiosignalspaningen radioteknisk kommunikationsspaning (COMINT), teknisk signalspaning (ELINT) och inhämtning genom avlyssning av instrumenteringssignaler från främmande utrustning (FISINT).

Signalspaningen riktar sig typiskt mot den interna signalkommunikationen mellan myndigheterna i en främmande stat eller t.ex. mot signalkommunikationen inom en trupp som utgör ett hot mot en finländsk fredsbevarande styrka. Den signalkommunikation som är föremål för signalspaning kan också vara digital datatrafik som överförs via radiosignaler. Av de radiofrekvensområden som stater förfogar över har i allmänhet vissa frekvenser reserverats enkom för de beväpnade styrkornas bruk, och den kommunikation som förekommer på dessa frekvensområden kan inte anses omfattas av skyddet för privata meddelanden. Främmande staters försvar kan i vilseledande syfte använda också andra frekvensområden i sin kommunikation än de som reserverats för dem.

Med teknisk signalspaning avses spaning mot och infångande, lokalisering och lagring av signaler som innehåller annat än kommunikation samt analysering av denna information. Sådana är t.ex. radarsignaler, höjdmätningssignaler och andra motsvarande signaler.

Instrumenteringssignaler från främmande utrustning är t.ex. sådana radiosignaler mellan delar i vapensystem som hänför sig till systemets funktion eller till övervakningen av systemets funktion. Olika tekniska anordningar och system kan kommunicera sinsemellan över radiovågorna, utan att det är fråga om kommunikation mellan två människor. Det kan t.ex. vara fråga om datautbyte mellan två anordningar, såsom att en robot styrs till sitt givna mål eller att ett vapensystem styrs från en kontrollcentral lägre bort. Det kan också vara fråga om någon annan verksamhet som grundar sig på radiovågor, såsom flygplans och robotars rörelser och mätningen av deras rörelse.

Enligt 136 § 3 mom. i lagen om tjänster inom elektronisk kommunikation får elektroniska meddelanden och förmedlingsuppgifter behandlas med kommunikationsparternas samtycke eller om så föreskrivs i lag. Genom den bestämmelse som behandlas i denna proposition föreskrivs det om underrättelseinhämtning som riktas mot radiovågor. Såsom det framgår av det föreslagna 2 mom. är en förutsättning för användning av metoden för underrättelseinhämtning en allmän förutsättning för användning av metoder för underrättelseinhämtning. Med stöd av den allmänna förutsättningen för användning av metoder för underrättelseinhämtning får radiosignalspaning användas enbart för inhämtande av information om den verksamhet som är föremål för underrättelseuppdraget.

I det föreslagna 2 mom. föreskrivs det separat om att radiosignalspaningen riktas mot objekt utanför finskt territorium. Om objektet kommer in på finskt territorium kan man gripa in och följa det bl.a. med stöd av befogenheterna i territorialövervakningslagen och med andra metoder för underrättelseinhämtning. Med de metoder som används inom radiosignalspaning ska man också i Finland kunna mäta de radiovågor som sänds av tekniska anordningar som används av landets egna och av vänligt sinnade styrkor, bl.a. i syfte att säkerställa funktionen hos tekniska anordningar och att komplettera de databaser och anordningar som hänför sig till egenskyddet. När metoden används i detta syfte är den dock inte en del av befogenheten för radiosignalspaning.

En förutsättning för radiosignalspaning är den allmänna förutsättningen för underrättelseverksamhet: att man med den med fog kan antas få information som behövs med tanke på ett underrättelseuppdrag.

I det föreslagna 3 mom. finns en informativ bestämmelse om att man med radiosignalspaning inte ska få inhämta information om innehållet förtrolig kommunikation mellan personer, vilket innebär att man med radiosignalspaning ska få inhämta information t.ex. om statliga aktörers meddelanden inom militär verksamhet.

Radiosignalspaning kan, beroende på verksamhetens natur och de metoder som används, inhämta radiosignaler som innehåller kommunikation som omfattas av sekretessen i fråga om förtroliga meddelanden. Ett sådant meddelande ska dock omedelbart förstöras i enlighet med de nedan avsedda skyldigheterna att förstöra material när informationens natur står klar. Bestämmelser om skyldigheten att förstöra material finns i 82 §. De upptagningar som uppkommit vid radiosignalspaning ska granskas på det sätt som föreskrivs i 107 §.

På finskt territorium har militärunderrättelsemyndigheten befogenheter till underrättelseinhämtning som avser person, med stöd av vilka myndigheten, om situationen kräver det, kan ingripa mot förtrolig kommunikation mellan två personer.

**59 §.** *Beslut om radiosignalspaning.* Enligt den föreslagna paragrafen ska beslut om radiosignalspaning fattas av Huvudstabens underrättelsechef. På grund av radiosignalspaningens natur ska det inte vara nödvändigt att fatta beslut om beslutets giltighetstid.

Dessutom är radiosignalspaning långvarigt och riktas i stor utsträckning mot verksamhetsfältet för en främmande stats beväpnade styrkor och det är även därför motiverat att inte ange någon giltighetstid för ett beslut om radiosignalspaning.

**60 §.** *Underrättelseinhämtning som avser utländska datasystem.* I paragrafen föreskrivs det om underrättelseinhämtning som avser utländska datasystem. Enligt 1 mom. får militärunderrättelsemyndigheten, när den finns i Finland, göra intrång i ett datasystem och ett datanät utanför Finland i syfte att inhämta information. Inhämtandet av information sker med datatekniska metoder.

Till skillnad från de ovan avsedda befogenheterna för teknisk observation av utrustning, teknisk avlyssning, teleavlyssning och teleövervakning ska det vid underrättelseinhämtning som avser utländska datasystem vara fråga om ett omfattande och långvarigt inhämtande av information från utländska datasystem och datanät. Underrättelseinhämtning som avser utländska datasystem har dock samma element som används vid inhämtandet av information som även finns i de ovannämnda befogenheterna, som anses som personbaserad underrättelseinhämtning, såsom avlyssning av tangentbordet, observation av interaktionen mellan en teknisk anordning och en person med hjälp av en datateknisk metod samt inhämtande av information från kommunikationssystem. Det är dock mest ändamålsenligt att föreskriva om verksamheten som en helhet med tanke på dess utrikespolitiskt känsliga natur. I det föreslagna nya 5 a kap. i polislagen finns det inte separata bestämmelser om underrättelseinhämtning som avser utländska datasystem, så i stället för underrättelseinhämtning som avser utländska datasystem används där metoderna teknisk avlyssning och teknisk observation av utrustning.

Den underrättelseinhämtning som avser datasystem är teknikneutral i förhållande till objektet, vilket innebär att underrättelseinhämtning som avser datasystem kan riktas inte bara mot datorer utan också mot andra motsvarande tekniska anordningar. Underrättelseinhämtningen kan också inbegripa inhämtande av information om en funktion i en anordnings programvara, lagrad information eller identifieringsuppgifterna i en anordning samt avlyssning, upptagning eller annan behandling av ett meddelande som inte är avsett för utomstående.

Det väsentliga är att man med anordningen behandlar information som kan vara av betydelse för underrättelseuppdraget och inhämtandet av information inom den militära underrättelseinhämtningen. De metoder som används inom den underrättelseinhämtning som avser utländska datasystem kan i realtid av en tjänsteman riktas t.ex. mot en viss programvara som används i ett informationssystem eller mot handlingar som lagras i systemet. De metoder som används inom den underrättelseinhämtning som avser utländska datasystem kan riktas exakt mot ett visst mål i ett datasystem, vilket också bidrar till att minska mängden information som inhämtas i onödan och inhämtandet av sådan information som är överflödig med tanke på användningen av befogenheten.

Med tanke på användningen av befogenheten är det inte ändamålsenligt att inhämta all information som finns i ett visst datasystem eller att inhämta sådan information som en sporadisk användare har sparat i datasystemet. En viktig aspekt när det gäller användningen av befogenheten är att användningen sker i hemlighet för den som metoden riktar sig mot. Dessutom kan inhämtandet av stora mängder information äventyra användandet av befogenheten i

hemlighet, eftersom den aktör som är föremål för användningen av metoden för underrättelseinhämtning kan märka en stor mängd datatrafik.

Befogenheten ska också vara neutral i förhållande till föremålet, och den kan riktas t.ex. mot uppgifter i handlingar som sparats i ett datasystem och mot sända meddelanden.

Den föreslagna fullmakten medför ingen skyldighet för finländska privata aktörer att installera s.k. bakdörrar i programvara och anordningar, och privata aktörer är inte heller skyldiga att lämna ut krypteringsnycklar.

Vid underrättelseinhämtning som avser datasystem ska det inte vara fråga om angripande verksamhet som har som syfte att ingripa i målsystemets funktion, utan det ska vara fråga om inhämtande av uppgifter som finns i datasystem, som lagras i datasystem och som produceras med hjälp av datasystem. Uppdragen kan dock vara förenade med utrikespolitiska aspekter som kräver noggrant övervägande.

I den folkrättsliga diskussionen särskiljer man vanligen mellan å ena sidan datasystemsoperationer som betjänar informationsinhämtningen och å andra sidan skadliga nätangrepp. Det har framförts olika synpunkter på om informationsinhämtning som riktas mot eller redan blotta närvaron i en annan stats datasystem ska tolkas som en kränkning av suveräniteten. Stater kan utifrån sin suveränitet reagera på en avslöjad informationsinhämtning på det sätt de finner lämpligt.

Enligt det föreslagna 2 mom. ska Försvarsmaktens underrättelsetjänst få inrikta underrättelseinhämtning som avser utländska datasystem på ett datasystem, om detta kan antas vara av synnerlig vikt för att inhämta information med avseende på ett underrättelseuppdrag. Momentet avgränsar ur vems datasystem och i vilka situationer information kan inhämtas. Militärunderrättelsemyndigheten har inte rätt att fritt släppa ut t.ex. sabotageprogram som skapar bakdörrar i datasystem och fritt använda sådana bakdörrar i slumpmässiga datasystem vid sin informationsinhämtning.

Tröskeln att använda befogenheten motsvarar den vid teknisk avlyssning och teknisk observation av utrustning, som bägge ligger nära verksamheten i fråga.

I fråga om andra än statliga aktörer är ett ytterligare krav att den verksamhet som är föremål för underrättelseinhämtning medför allvarlig fara för den nationella säkerheten.

Enligt det föreslagna 3 mom. ska det upprättas en skriftlig plan över genomförandet av underrättelseinhämtning som avser utländska datasystem. Av planen ska det framgå på vilket sätt intrånget i datasystemet i fråga görs och på vilket sätt eventuella risker med användningen av metoden för underrättelseinhämtning har beaktats.

Det datasystem som är föremål för metoden för underrättelseinhämtning kan inte nödvändigtvis anges särskilt noggrant på förhand. Av den anledningen kan föremålet för metoden för underrättelseinhämtning anges mindre detaljerat än t.ex. i samband med teknisk observation av utrustning. Utifrån den information som redan inhämtats kan planen sedan specificeras och metoden för underrättelseinhämtning riktas exakt mot ett visst föremål.

Med tanke på karaktären av metoden för underrättelseinhämtning har den tjänsteman som använder metoden inte nödvändigtvis exakt information om var i det datasystem som är föremålet den information som behövs för ett underrättelseuppdrag finns lagrad. Medan en metod för

underrättelseinhämtning används kan den tjänsteman som använder metoden styra den programvara som används för informationsinhämtningen utifrån information som redan inhämtats så att den riktas mot information i en viss, betydelsefull del av datasystemet.

I planen ska det också på en övergripande nivå beskrivas vilken typ av information som man antar att kan inhämtas ur datasystemet och vilken information man avser inhämta ur det. Med tanke på karaktären av metoden för underrättelseinhämtning kan all information i datasystemet inte lagras, utan den tjänsteman som använder metoden ska aktivt kunna påverka vilken information som inhämtas.

**61 §.** *Beslut om underrättelseinhämtning som avser utländska datasystem.* I det föreslagna 1 mom. föreskrivs det om beslutsfattande vid underrättelseinhämtning som avser datasystem i situationer som inte inbegriper utrikes- eller säkerhetspolitiskt betydande kopplingar. Beslut om underrättelseinhämtning som avser datasystem ska fattas av Försvarsmaktens underrättelsechef. Huvudstabens underrättelsechef ska beakta de principer som avses i det föreslagna 1 kap. i sitt eget beslutsfattande och t.ex. bedöma om användningen av metoden för underrättelseinhämtning står i rätt proportion till den information som inhämtas.

Eftersom den underrättelseinhämtning som avser utländska datasystem i praktiken gäller inhämtande av information ur ett datasystem utanför Finlands gränser motsvarar beslutsnivån den som gäller för militär underrättelseinhämtning som sker utomlands.

För att säkerställa en tillräcklig samhällelig acceptans i sådana situationer ska Försvarsmaktens underrättelsechef, efter att ha utvärderat situationen och innan han eller hon fattar beslut om inledande av underrättelseinhämtning som avser utländska datasystem, föra ärendet till samordningsgruppen för underrättelse för behandling. En bedömning av behovet att behandla ärendet samordnat mellan de myndigheter som avses i 14 § ska göras av Huvudstabens underrättelsechef. I 2 mom. föreskrivs det om ett beslut om underrättelseinhämtning som avser utländska datasystem.

Enligt den föreslagna 2 punkten ska i beslutet nämnas föremålet för åtgärden. Med tanke på karaktären av metoden för underrättelseinhämtning kan föremålet inte nödvändigtvis beskrivas lika noggrant som i samband med teknisk avlyssning och teknisk observation av utrustning. Målet ska ändå beskrivas med tillräcklig noggrannhet, så att användningen av metoden för underrättelseinhämtning inte fullständigt okontrollerat ger information om all information i ett visst datasystem. Användningen av metoden för underrättelseinhämtning är dessutom sådan att all information om datasystemet inte lagras.

Enligt den föreslagna 3 punkten ska i beslutet nämnas målet och genomförandeplanen för underrättelseinhämtning som avser utländska datasystem. Punkten är väsentlig eftersom den underrättelseinhämtning som avser utländska datasystem på det sätt som beskrivs ovan i detaljmotiveringen till 61 § ska vara planenlig verksamhet. Försvarsmaktens underrättelsetjänst har inte rätt att i informationsnäten släppa ut programvara som helt okontrollerat inhämtar information, utan den programvara som används för informationsinhämtning ska riktas mot ett visst föremål enligt 2 punkten. Det datasystem mot vilket den programvara som används för informationsinhämtningen riktas kan ändras, och den tjänsteman som använder metoden för informationsinhämtning har inte nödvändigtvis vetskap om i vilken del av datasystemet vilken information finns lagrad. Utifrån de uppgifter som inhämtats medan metoden för underrättelseinhämtning används ska planen vid behov ses över.

Enligt det föreslagna 3 mom. ska försvarsministeriet hållas informerat om pågående underrättelseinhämtning. Försvarsministeriet kan enligt prövning informera andra viktiga, utrikes- och säkerhetspolitiskt betydelsefulla aktörer, såsom utrikesministern och republikens president.

**62 §.** *Militär underrättelseinhämtning utomlands.* I paragrafen föreskrivs det om användningen av metoder för underrättelseinhämtning utanför Finlands gränser. Vissa metoder för underrättelseinhämtning, såsom underrättelseinhämtning som avser datatrafik och underrättelseinhämtning som avser utländska datasystem, är redan till sin natur sådana att det inte är ändamålsenligt att fatta beslut om dem med stöd av denna paragraf.

Enligt det föreslagna 1 mom. kan på militär underrättelseinhämtning utomlands och på användning av metoder för underrättelseinhämtning utomlands tillämpas, utöver vad som föreskrivs om förbud mot underrättelseinhämtning som gäller ett utrymme som används för stadigvarande boende, bestämmelserna i 58 § 3 mom., 76, 77, 79 och 80 §, 82 § 2 mom., 84 och 86 §.

Militärunderrättelsemyndighetens prövningsrätt och användning av metoder för underrättelseinhämtning även vid utländska förhållanden styrs av de allmänna principerna i denna lag, och deras betydelse för den militära underrättelseinhämtningen behandlas närmare i samband med detaljmotiveringen till de paragrafer som gäller dessa. Dessutom har tillgodoseendet av de grundläggande och mänskliga rättigheter som föreskrivs i förvaltningslagen, som särskilt förpliktar tjänstemän, en viktig roll när det gäller underrättelseinhämtning som avser utländska förhållanden. När det är fråga om underrättelseinhämtning som avser utländska förhållanden kan bestämmelserna i Europakonventionen till en del utgöra tolkningsgrund, särskilt när målstatens rättssystem, kultur och omständigheter inte motsvarar de västerländska. En människorättsbaserad motivering kan användas som ett hjälpmedel för att styra tolkningen i fråga om den underrättelseinhämtning som avser utländska förhållanden.

Av grundlagens 2 § 3 mom. och 22 § följer att en finländsk tjänsteman inte heller utomlands kan förfara på ett sätt som kränker de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. Med hänsyn till att den underrättelseinhämtning som avser utländska förhållanden är känslig till sin natur är det dock i enskilda fall motiverat att det moment och den paragraf som nämns separat i det föreslagna momentet inte alltid behöver tillämpas. Detta framhävs av formuleringen ”kan tillämpas”. Detta ger Huvudstabens underrättelsechef prövningsrätt att bedöma när bestämmelserna kan tillämpas och när det inte är motiverat att tillämpa dem.

I de bestämmelser som gäller metoder för underrättelseinhämtning föreskrivs ett förbud mot att rikta metoder för underrättelseinhämtning mot ett utrymme som används för stadigvarande boende. Utgångspunkten är att man inte ens i fråga om underrättelseinhämtning som avser utländska förhållanden kan rikta informationsinhämtningen mot någons bostad. Gränsdragningen kan vid underrättelseinhämtning som avser utländska förhållanden vara nästintill omöjlig, i synnerhet när i fråga om utrymmen som används för stadigvarande boende i situationer där underrättelseinhämtningen sker i ett mindre utvecklat eller underutvecklat land där infrastrukturen inte möjliggör utredande av bostadens användningsändamål t.ex. ur myndighetsregister.

Det i bestämmelsen nämnda 58 § 3 mom. gäller en begränsning av radiosignalspaningen och enligt det momentet ska information inte få inhämtas med radiosignalspaning om innehållet i andra än statliga aktörers meddelanden. Vid underrättelseinhämtning som avser utländska förhållanden är en motsvarande begränsning inte motiverad. Särskilt inom Försvarsmaktens internationella verksamhet kan det uppstå situationer där ett sådant hot riktas mot Försvarsmak-

ten som inte kommer från statligt håll, t.ex. terrorism vid en militär krishanteringsinsats. Dessutom är det inte nödvändigtvis möjligt att i alla situationer utnyttja teleavlyssning utomlands.

I ovannämnda situationer kan det vara motiverat att rikta radiosignalspaning mot någon annan än en statlig aktör för att reda ut innehållet i ett meddelande. Det väsentliga när det gäller radiosignalspaning är att identifiera att den signal som är föremål för radiosignalspaningen sänds och tas emot utanför Finlands gränser eller att radiosignalen är utanför Finlands gränser när radiosignalspaningen riktas mot den.

Radiosignalspaning utomlands hänger också nära samman med bestämmelsen i 82 § 2 mom., enligt vilken radiosignalspaningen ska avbrytas omedelbart och upptagningarna och anteckningarna utplånas, till den del det framgår att den gäller innehållet i ett meddelande från någon annan än en statlig aktör. I Försvarsmaktens internationella verksamhet kan hot riktas mot Försvarsmakten även från andra än statliga håll, och därför kan det inte i alla situationer anses ändamålsenligt att tillämpa bestämmelsen i 82 § 2 mom.

I den föreslagna 76 § föreskrivs det om utlämnande av uppgifter om brott och i 77 § om utlämnande av uppgifter i vissa fall. Bestämmelserna i bägge paragraferna är också efter prövning tillämpliga på underrättelseinhämtning som avser utländska förhållanden.

I den föreslagna 79 § föreskrivs det om förbud mot underrättelseinhämtning och i 80 § om kopieringsförbud, och dessa bestämmelser är också efter prövning tillämpliga på underrättelseinhämtning som avser utländska förhållanden.

I den föreslagna 84 § föreskrivs det om utplåning av uppgifter som fåtts i en brådskande situation. Bestämmelsen är inte tillämplig på underrättelseinhämtning som avser utländska förhållanden, eftersom Huvudstabens underrättelsechef utan undantag ska fatta beslut om användningen av varje metod för underrättelseinhämtning.

I den föreslagna 86 § föreskrivs det om underrättelse om användning av en metod för underrättelseinhämtning. I 86 § 1 mom. föreskrivs det om skyldigheten att ge en underrättelse om användningen av de i momentet nämnda metoderna för underrättelseinhämtning till den person som varit föremål för dem efter det att syftet med användningen av metoden har nåtts. Att underrätta föremålet för användningen av en metod för underrättelseinhämtning vid underrättelseinhämtning som avser utländska förhållanden skulle avslöja användningen av underrättelseverksamhet på en annan stats territorium, vilket skulle kunna skada relationerna mellan staterna. Detta talar för att inte göra någon underrättelse eftersom en finsk domstol varken har behörighet att fatta beslut om att underrättelse om användning av en metod för underrättelseinhämtning vid underrättelseinhämtning som avser utländska förhållanden ska skjutas upp eller helt utebli eller att besluta om användning av en metod för underrättelseinhämtning. Således görs bedömningen av beslut som gäller underrättelse av militärunderrättelsemyndigheten ensam.

Enligt det föreslagna 2 mom. ska beslut om militär underrättelseinhämtning och användning av metoder för underrättelseinhämtning som sker utanför Finland fattas av Huvudstabens underrättelsechef. Med andra ord är det Huvudstabens underrättelsechef som på operativ nivå ska fatta beslut om militär underrättelseinhämtning som sker utanför Finland och om de metoder för underrättelseinhämtning som används i samband med den. Med hänsyn till att den underrättelseinhämtning som avser utländska förhållanden är förknippad med utrikespolitiskt känsliga aspekter måste man i beslutsfattandet beakta underrättelseinhämtningens fokusering samt bestämmelserna i 14 § och de riktlinjer som eventuellt följer av dem.

Enligt det föreslagna 3 mom. ska i fråga om innehållet i ett beslut, en framställning och en plan som gäller användning av en metod för underrättelseinhämtning iakttas vad som i den föreslagna lagen föreskrivs om framställningar, planer, tillstånd eller beslut.

I ett beslut som gäller användning av en metod för underrättelseinhämtning utanför Finland ska nämnas motsvarande uppgifter som i en framställning, en plan, ett yrkande eller ett beslut när metoden för underrättelseinhämtning används i Finland.

*Informationsinhämtning som avser datatrafik*

Underrättelseinhämtning är i sin helhet verksamhet som syftar till att förutse kommande händelser och att så tidigt som möjligt identifiera sådana hot som riktas mot Finland och som hänför sig till uppgifter inom militär underrättelseinhämtning. Föremålet för underrättelseverksamheten utgörs framför allt av främmande staters organisationer och deras aktörer.

Underrättelseinhämtning som avser datatrafik är en del av den militära underrättelseinhämtningen och av den underrättelseverksamhet som den militära underrättelseinhämtningen utför. Underrättelseinhämtning som avser datatrafik går ut på att ur den datatrafik som rör sig inom Finland automatiserat samla in och lagra datatrafik som förekommer i den del av kommunikationsnätet som motsvarar tillståndsvillkoren, såsom enligt datakabelns fibervåglängd, i enlighet med de angivna sökbegreppen. Till skillnad från underrättelseinhämtning som avser en främmande stats datatrafik sker den underrättelseinhämtning som avser datatrafik inom Finland och den riktas mot datatrafik inom Finland som överskrider Finlands gräns. Av denna orsak kan föremålet för underrättelseinhämtning som avser datatrafik vara t.ex. sådan kommunikation som till följd av datatrafikens leveransväg tillfälligt finns inom Finlands gränser. Inom underrättelseinhämtning som avser datatrafik letar man målinriktat efter för underrättelseuppdraget väsentliga uppgifter bland en stor mängd information.

Med hjälp av underrättelseinhämtning som avser datatrafik kan omfattande information fås om föremålet för den militära underrättelseinhämtningen. Med hjälp av underrättelseinhämtning som avser datatrafik kan uppgifter fås ur telefonsamtal, epostmeddelanden, direktmeddelanden och andra motsvarande kommunikationskanaler och kommunikationsmetoder. Uppgifter som är viktiga för militär underrättelseinhämtning kan förmedlas av vem som helst inom den organisation eller grupp av aktörer som är föremål för den militära underrättelseinhämtningen. I den helhet som utgörs av den militära underrättelseverksamheten kan de uppgifter som inhämtas med hjälp av underrättelseinhämtning som avser datatrafik bestå t.ex. av uppgifter om var föremålet för ett underrättelseuppdrag finns, var det rör sig, om dess sammansättning samt om organisationer som anknyter till föremålen för den militära underrättelseinhämtningen, såsom om aktörer som stöder militära organisationer i en främmande stat.

När det gäller inriktning av underrättelseinhämtning som avser datatrafik ska datatrafiken styras från den del av ett kommunikationsnät som tillståndet gäller, t.ex. enligt fibervåglängd, vidare till den militära underrättelseinhämtningen, som ska ha rätt att för den behandling som militärunderrättelsemyndigheten gör inhämta och lagra sådana meddelanden som uppfyller de villkor som anges i domstolens tillstånd. I den här fasen styrs uppgifterna till cacheminnet för det system som används för underrättelseinhämtning som avser datatrafik, där behandlingen av informationen är tillfällig och temporär. Användningen av ett cacheminne är en oskiljaktig och nödvändig del av systemets tekniska process, vars syfte är att ur datakommunikationsflödet finna meddelanden som stämmer överens med sökbegreppen. Datakommunikation som inte motsvarar sökbegreppen saknar självständig betydelse för underrättelseuppdraget. Militärunderrättelsemyndigheten kan inte lagra den information som finns i cacheminnet separat,

om den inte motsvarar de sökbegrepp som angetts i tillståndet från domstolen. Med hänsyn till cacheminnets syfte lagras uppgifterna där en synnerligen kort tid, i praktiken är det fråga om sekunder, innan de skrivs över av ny information som kommer in i cacheminnet.

Underrättelseombudsmannen ska övervaka användningen av underrättelseinhämtning som avser datatrafik. Underrättelseombudsmannen ska också övervaka att de tekniska lösningar som används är lämpliga och att underrättelsemyndigheten inte strävar efter att kringgå lagen t.ex. genom att göra det tekniskt möjligt att använda cacheminnet så att de uppgifter som passerat det kan tas fram senare.

Sökbegreppen får inte riktas mot innehållet i meddelandena när de samlas in och lagras. Först i samband med att meddelandena behandlas ska militärunderrättelsemyndigheten ha rätt att behandla innehållet i meddelandena och andra uppgifter som hänför sig till dem. Militärunderrättelsemyndigheten ska inte ha rätt att behandla någon annan datatrafik än den som har lagrats med stöd av domstolens tillstånd. Sådan datatrafik och sådana meddelanden som inte motsvarar de sökbegrepp som anges i domstolens tillstånd ska i samband med den automatiska inhämtningen och lagringen avlägsnas ur den process som gäller underrättelseverksamhet och underrättelseinhämtning som avser datatrafik. Datatrafik som inte motsvarar kategorierna av sökbegrepp och sökvillkoren får inte i efterhand tas fram för att användas av underrättelsemyndigheten. Den underrättelseinhämtning som avser datatrafik hänför sig alltid till ett visst underrättelseuppdrag och den kan endast användas under den tidsperiod som anges i domstolens tillstånd.

Datatrafik som lagrats på basis av sökbegreppen ska vara en del av utövandet av befogenheten. Granskningen av insamlad datatrafik omfattas i likhet med andra metoder för underrättelseinhämtning av den skyldighet att granska upptagningar och handlingar som avses i den föreslagna 107 §.

I samband med att meddelandena behandlas tar man ur kommunikationen fram uppgifter till stöd för underrättelsemyndighetens analyser och rapporter samt samlar man in annan, för underrättelseuppdraget viktig information till att användas t.ex. för vidare inriktning av metoderna för underrättelseinhämtning. I samband med detta klarnar det också vilken del av uppgifterna som är personuppgifter som ska behandlas på det sätt som föreskrivs i lagen om behandling av personuppgifter inom Försvarsmakten, och vilken del som är annat än personuppgifter. Behandlingen av personuppgifter övervakas av dataombudsmannen och för sin del av underrättelseombudsmannen. Ur det material som motsvarar sökvillkoren ska man dessutom utplåna sådant material som omfattas av förbud mot underrättelseinhämtning och material som omfattas av skyldigheten till omedelbar utplåning.

Syftet med underrättelseinhämtning som avser datatrafik är att inhämta väsentlig information om den datatrafik som föremålet för underrättelseuppdraget har, inte t.ex. att via inhämtandet av förmedlingsuppgifter som anknyter till enskilda personer skapa en bredare profil om personens beteende.

Underrättelseinhämtning som avser datatrafik kan även riktas mot uppgifter som finns lagrade i molntjänster. Det primära syftet med den underrättelseinhämtning som avser datatrafik är att inhämta information om den verksamhet som är föremål för den militära underrättelseinhämtningen och att identifiera de aktörer och personer som ligger bakom den. Den underrättelseinhämtning som avser datatrafik som görs i fråga om lagring i molntjänster har motsvarande betydelse som annan underrättelseinhämtning som avser datatrafik för att fullfölja detta syfte. Lagring i molntjänster utnyttjas i själva verket i hög grad t.ex. i verksamhet som anknyter till

spionage. Exempelvis genomförs statligt cyberspionage vanligen så att det sabotageprogram som används vid spionaget lagrar den information den kommer åt på en server i en molntjänst i utlandet. Dessutom använder många direktmeddelandetjänster molntjänster för att förmedla kommunikationen.

Sökvillkor som riktas mot molntjänster ska få användas på samma grunder som andra sökvillkor, alltså förutsatt att domstolen i sitt beslut godkänner användningen av dem. Ett sökvillkor som används i fråga om lagring i molntjänster ska alltid grunda sig på ett tillräckligt konkret föremål för den militära underrättelseinhämtningen och Försvarsmaktens underrättelsetjänst ska vara skyldig att lägga fram fakta om detta föremål i det yrkande på tillstånd som den framför till domstolen.

En oskiljaktig del av den underrättelseinhämtning som avser datatrafik är även behandlingen av de tekniska uppgifterna om kommunikationen och med det avses andra än innehållsliga uppgifter om de meddelanden som rör sig i kommunikationsnäten. Sådana uppgifter är bl.a. meddelandets identifikationsuppgifter. Med detta säkerställs det att den underrättelseinhämtning som avser datatrafik riktas så exakt som möjligt till rätt del av kommunikationsnätet.

Vid underrättelseinhämtning som avser datatrafik kan man dessutom inhämta information om var en teknisk anordning eller terminalutrustning finns.

**63 §.** *Behandling av tekniska data.* I paragrafen ska det föreskrivas om Försvarsmaktens underrättelsetjänsts rätt att samla in och lagra tekniska data om datatrafiken i ett kommunikationsnät samt med hjälp av automatisk databehandling behandla dem för statistisk analys för att den underrättelseinhämtning som avser datatrafik ska kunna utvecklas och mera exakt inriktas på den aktuella delen av kommunikationsnätet. De tekniska data gäller teleföretag och dataöverförare som använder förbindelserna och förmedlar kommunikationen samt andra organisationer såsom strömningstjänster.

De data som inhämtas är av betydelse när underrättelseinhämtning som avser datatrafik inriktas på det sätt som föreskrivs i 65 och 67 §.

Kommunikationens tekniska data gäller inte innehållet i ett meddelande. Genom behandling av tekniska data får man information om datatrafikflödena i ett datatrafiknät och en uppfattning till exempel om i vilken del av kommunikationsnätet det flödar datatrafik till och från ett visst geografiskt område. Med hjälp av behandlingen av tekniska data kan man bättre inrikta underrättelseinhämtning som avser datatrafik endast på de delar av kommunikationsnätet, där det flödar kommunikation som är väsentlig med tanke på ett underrättelseuppdrag. Genom analys av tekniska data kan man inhämta mera exakta uppgifter för ansökan om tillstånd till underrättelseinhämtning som avser datatrafik och för den fysiska inriktningen på en viss del av kommunikationsnätet.

Med kommunikationens tekniska data avses bl.a. förmedlingsuppgifter om meddelandena. Datatrafikens tekniska data definieras i 9 § 8 punkten i denna lag. Andra tekniska data om kommunikationen kan vara BGP-dirigeringsuppgifter (Border Gateway Protocol), IP-adressområden och numret på det autonoma systemet (AS-numret).

Vid behandlingen av kommunikationens tekniska data strävar man efter att reda ut i vilken del av ett kommunikationsnät en viss aktörs datakommunikation eller datakommunikationen till och från ett visst geografiskt område löper. Detta kan göras t.ex. genom att man först ur de officiellt tillgängliga uppgifterna inhämtar BGP-dirigeringen av kommunikationen, av vilken

framgår ägarna till de autonoma system genom vilka kommunikation flödar fram till en viss punkt.

I typiska fall är ägarna till de autonoma systemen operatörer och andra större aktörer, vilka ansvarar för dirigeringshelheter för vissa IP-adressområden. De autonoma systemen specificeras med s.k. AS-nummer. I första hand innehas AS-nummer av teleföretag, allt från lokala teleföretag till globala förmedlare av datakommunikation, IKT-tjänstetillhandahållare samt stora, globala företag. Via AS-numren kan man specificera vissa IP-adressområden, som administreras av innehavaren av AS-numret och distribueras vidare till kunderna för att användas av dem.

Utgående från IP-adressområdena kan aktörer som är väsentliga för ett underrättelseuppdrag och ett visst område som datakommunikation flödar från och till identifieras i datakommunikationen.

Genom behandling av tekniska data strävar man redan i utgångsläget efter att avgränsa sådan datakommunikation som är irrelevant och utesluta den från den underrättelseinhämtning som avser datatrafik. Enligt olika uppskattningar används över 60 procent av kapaciteten i kommunikationsnätet för datatrafik som förmedlar olika slag av strömningstjänster och av denna datatrafik är största delen videobilder. Vidare hänför sig en betydande del av den använda kapaciteten i kommunikationsnätet också till annan nöjesanvändning, såsom datorspel och nätthandel.

I princip kan den datakommunikation som hänför sig till de tjänster som nämns ovan anses vara irrelevant med tanke på militär underrättelseinhämtning. I de flesta fall kan det behov av underrättelseinhämtning som anknyter till videobilder uppfyllas också med andra metoder för underrättelseinhämtning än underrättelseinhämtning som avser datatrafik, såsom en täckoperation i datanät.

Insamlade och lagrade tekniska data om kommunikationen ska genomgå en statistisk analys med hjälp av automatisk databehandling. Utifrån denna statistiska analys kan insamlandet och lagrandet av kommunikation bättre inriktas fysiskt endast på den del av kommunikationsnätet, där det förmodas röra sig kommunikation som är väsentlig med tanke på ett underrättelseuppdrag.

Vidare kan man med den statistiska analysen få mera exakta uppgifter för den ansökan om tillstånd som gäller insamlande och lagrande av datatrafik.

I enlighet med 1 mom. ska med kortvarig lagring avses att behandlingen av tekniska data ska försiggå under en kort tid. Som grund för en statistisk analys ska man kunna samla in tekniska data antingen genom att ta ett kortvarigt prov på hela datakommunikationsflödet eller genom att som grund för den statistiska analysen ta t.ex. vart tiotusende IP-paket ur datakommunikationsflödet. I båda fallen ska den statistiska analysen grunda sig på sporadiska IP-paket i datakommunikationsflödet. I den plan över behandlingen av tekniska data som ska presenteras för domstolen ska genomförandet av behandlingen av tekniska data beskrivas närmare. Om detta ska föreskrivas i 63 § 3 mom. 4 punkten.

Syftet med den statistiska analysen av tekniska data om kommunikationen är att reda ut om datakommunikation från eller till ett visst geografiskt område eller en viss aktör flödar i en viss del av kommunikationsnätet. Militärunderrättelsemyndigheterna ska inte få använda insamlade och lagrade tekniska data om kommunikationen för annat syfte än för statistisk analys

med hjälp av automatisk databehandling. En automatisk datateknisk statistisk analys ska göras omedelbart efter att de tekniska data har samlats in och lagrats, och efter detta ska de data som låg till grund för analysen omedelbart utplånas.

Vid behandlingen av tekniska data ska Försvarsmaktens underrättelsetjänst inte ha tillträde till enskilda tekniska data om kommunikationen och militärunderrättelsemyndigheten ska därmed inte kunna ta reda på en fysisk person som är part i kommunikationen.

Genom behandlingen av tekniska data ska man också kunna inhämta behövliga uppgifter om ändringar som sker i datakommunikationen. Hur datakommunikationen rör sig i kommunikationsnätet kan förändras också med korta intervall bl.a. till följd av ändringar i dirigeringen av kommunikationen, i teknikerna samt datatrafiktrådarna. För att den underrättelseinhämtning som avser datatrafik ska kunna inriktas så exakt som möjligt fysiskt och tekniskt, måste militärunderrättelsemyndigheten ha så aktuell information som möjligt om de tekniska omständigheter som inverkar på inriktningen, såsom om meddelandenas BGP-dirigering samt om de kommunikationsnätsdelar som vissa aktörer, såsom användarna av strömningstjänster, använder.

Genom en statistisk analys av kommunikationens tekniska data ska man inte kunna ta reda på en fysisk person som är part i kommunikationen eller meddelandets innehåll.

Försvarsmaktens underrättelsetjänst utför för skyddspolisens räkning det tekniska genomförandet av underrättelseinhämtning som avser datatrafik utgående från ett separat uppdrag från skyddspolisen. Skyddspolisen ska kunna ge Försvarsmaktens underrättelsetjänst i uppdrag att inhämta tekniska data, och underrättelsetjänsten ska i ett sådant fall skaffa det tillstånd som behövs och utföra en statistisk analys av tekniska data samt ställa analysen till skyddspolisens förfogande. Bestämmelser om tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning finns nedan.

I 2 mom. ska det föreskrivas om förbud mot att utgående från tekniska data om kommunikationen producera sådan information som kan användas för att identifiera enskilda fysiska personer. Syftet med förbudet är också att förhindra att befogenheten till underrättelseinhämtning som avser datatrafik som inriktas på personer kringgås. Avsikten med den statistiska analysen är att producera information om i vilken del av ett kommunikationsnät det flödar datatrafik från eller till ett visst objekt som är väsentligt med tanke på ett underrättelseuppdrag. Syftet med den statistiska analysen är att underrättelseinhämtning som avser datatrafik ska kunna inriktas fysiskt och tekniskt så exakt som möjligt på datatrafik som flödar endast i den del av ett kommunikationsnät som är väsentlig med tanke på ett underrättelseuppdrag. Genom fysisk och teknisk inriktning kan man utesluta en stor del av den datatrafik som rör sig i kommunikationsnäten och som inte har någon betydelse med tanke på uppdragen inom den militära underrättelseinhämtningen.

I 3 mom. ska ingå en skyldighet att förstöra tekniska data. Tekniska data som används vid behandlingen av tekniska data ska inte få lagras för användning senare inom den militära underrättelseinhämtningen. Avsikten är att vid behandlingen av tekniska data ska en statistisk analys produceras och efter detta ska de data som utgjort grund för analysen omedelbart förstöras och de ska inte kunna användas i efterskott för att utföra ett underrättelseuppdrag.

**64 §.** *Beslut om behandling av tekniska data.* Enligt 1 mom. ska beslut om behandling av tekniska data fattas av domstol på yrkande av en för uppdraget förordnad och med användningen

av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vid Försvarsmaktens underrättelsetjänst. Bestämmelser om förfarandet i domstol finns nedan.

Enligt 2 mom. ska den maximala giltighetstiden för ett tillstånd som gäller behandling av tekniska data vara tre månader. På tillståndets giltighetstid ska inverka hur insamlandet av tekniska data genomförs. Insamlandet av tekniska data kan genomföras så att som föremål för en teknisk analys tas ett kortvarigt prov av all datatrafik i en viss del av kommunikationsnätet, varvid det är motiverat att tillståndet gäller en kortare tid eller så att t.ex. vart tiotusende paket av IP-paketen i en viss del av kommunikationsnätet tas, varvid tillståndets giltighetstid kunde vara längre.

I det första alternativet kan militärunderrättelsemyndigheterna under tillståndets giltighetstid i flera repriser kortvarigt samla in och lagra tekniska data om trafiken i ett kommunikationsnät och av dem genom automatisk databehandling producera en statistisk analys. I detta fall är det naturligt att tillståndets giltighetstid är kortare, eftersom datatrafik i mera vidsträckt bemärkelse blir föremål för teknisk analys, fastän det är fråga om kortvarigt insamlande och lagrande av data. I det senare alternativet ska tillståndet kunna gälla en längre tid, eftersom det är fråga om att ta sporadiska IP-paket för teknisk analys. I detta alternativ blir datatrafiken inte i lika stor omfattning som i det första alternativet föremål för teknisk analys under en viss tidpunkt, vilket motiverar en längre giltighetstid för tillståndet.

Enligt 3 mom. 1 punkten ska i ansökan om tillstånd i första hand anmälas det geografiska område i fråga om vilket tekniska data i inkommande eller utgående datatrafik ska redas ut. Det geografiska området ska enligt behov kunna vara ett vidsträckt område, där man vet att det förekommer t.ex. militär verksamhet, eller en viss byggnad som man vet att har samband med ett underrättelseuppdrag. Men området kan också vara ett område i Finland som är viktigt t.ex. med tanke på energiinfrastrukturen och i fråga om vilket det kan behöva göras en analys av inkommande datatrafikflöden till följd av ett hot som riktar sig mot samhällets vitala funktioner.

Dock kan man inte alltid namnge ett specifikt geografiskt område som källa till eller föremål för trafik. De digitala tjänsterna byggs allt mera så att de är oberoende av en fysisk plats. En part som agerar fientligt kan t.ex. styra de informationssystem som används vid en attack från en molntjänst, och då kan det fysiska läget för de anordningar som ingår i den inte redas ut på förhand. Därför kan man i tillståndsansökan i stället för ett geografiskt område också använda ett nätområde för att avgränsa tillståndet, när man inte känner till det geografiska området eller det geografiska området skulle vara orimligt stort. Med nätområde ska avses en naturlig enhetlig datamängd som bildas av nätadresser. Ett nätområde kan vara ett s.k. autonomt dirigeringsområde (AS), en datamängd som bildas av IP-adresser eller ett s.k. domänområde, såsom mil.xy.

När ett områdes omfattning bedöms bör man uppmärksamma var man kan behöva sätta in underrättelseinhämtning på inkommande eller utgående datakommunikationsflöden. Det kan inte heller anses förenligt med proportionalitetsprincipen eller principen om ändamålsbundenhet att ansöka om tillstånd för analysering av i internet ingående eller utkommande datakommunikationsflöden för en helt summarisk storlek. En analys av datatrafikflöden från alla håll ger inte heller nödvändigtvis ett slutresultat som motsvarar syftet vad gäller att inrikta den underrättelseinhämtning som avser datatrafik.

Enligt momentets 2 punkt ska militärunderrättelsemyndigheten meddela de delar av kommunikationsnätet, såsom datakommunikationstrådens fiber, fiberns våglängd eller en annan mera

exakt dataöverföringsnivå, där tekniska data om datatrafiken kommer att samlas in. För att man i den helhet som kommunikationsnätet utgör ska kunna hitta den del som är väsentlig med tanke på underrättelseinhämtningen, måste insamlandet och lagrandet av tekniska data med samma tillstånd kunna inriktas på flera än en kommunikationsnätsdel.

Också antalet kommunikationsnätsdelar ska bedömas enligt proportionalitetsprincipen och principen om ändamålsbundenhet. Syftet med behandlingen av tekniska data är att producera en analys för att inrikta den underrättelseinhämtning som avser datatrafik. Det är inte förenligt med detta syfte att analysera datatrafikflödet i alla kommunikationsdelar som överskrider Finlands gräns för att kunna analysera den datatrafik som flödar till eller från ett visst område.

I momentets 3 punkt ska för insamlandet av tekniska data utses en tjänsteman vid Försvarsmaktens underrättelsetjänst som övervakar och leder behandlingen av tekniska data om kommunikationen och som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning. Den tjänsteman som övervakar och leder ska agera under tjänsteansvar i sitt uppdrag. Insamlandet, lagrandet och behandlingen av tekniska data ska övervakas av underrättelseombudsmannen, om vars uppgifter ska föreskrivas i en särskild lag.

Enligt 4 punkten ska i ansökan om tillstånd presenteras en plan för hur, när och under hur långa tidsintervall insamlandet och lagrandet av tekniska data ska genomföras. I planen ska också presenteras vilken metod som ska användas vid den tekniska analysen. I enlighet med det som beskrivs ovan ska den behandling av tekniska data som avses i paragrafen kunna genomföras genom att kortvariga prover, från en till några sekunder, tas på all datatrafik i en viss del av ett kommunikationsnät eller genom att t.ex. vart tiotusende IP-paket sporadiskt tas ur datatrafikflödet i kommunikationsnätsdelen.

I planen ska det anges med vilken av de ovan beskrivna metoderna tekniska data ska inhämtas. Eftersom behandlingen av tekniska data i datatrafiken ska kunna ske kortvarigt och inriktas på all datatrafik som rör sig i en kommunikationsnätsdel, är det ändamålsenligt att Försvarsmaktens underrättelsetjänst under den tid tillståndet gäller kunde samla in och lagra tekniska data flera gånger. I planen ska det också meddelas hur många gånger man har för avsikt att inhämta tekniska data under tillståndets giltighetstid.

Alternativt ska det i planen meddelas hur det sporadiska insamlandet av IP-paket ska genomföras.

Genomförandet av behandlingen av tekniska data ska bedömas genom proportionalitetsprincipen och principen om ändamålsbundenhet.

**65 §.** *Underrättelseinhämtning som avser en statlig aktörs datatrafik*. I paragrafen ska det föreskrivas om Försvarsmaktens underrättelsetjänsts befogenhet att samla in, lagra och behandla en statlig aktörs kommunikation samt om förutsättningarna för detta. Den statliga aktör som avses i paragrafen ska vara ett särskilt föremål jämfört med övrig underrättelseinhämtning som avser datatrafik.

Enligt gällande tolkning åtnjuter staten och övriga offentliga sammanslutningar inte skydd för de grundläggande fri- och rättigheterna (RP 309/1993 rd och GrUU 9/2015 rd), varvid inte heller den kommunikation som en stat bedriver kan anses åtnjuta det grundlagsenliga skyddet för hemligheten i fråga om förtroliga meddelanden.

Om insamlandet av datatrafik kunde inriktas enbart på en främmande stats datatrafik, kunde i de sökbegrepp som riktas mot denna också inbegripas data som beskriver meddelandets innehåll. Sökbegrepp kunde vara en teckensträng som finns i innehållet i meddelandet, t.ex. ett ord eller en sats i ett naturligt språk.

Tillämpningen av det undantag som gäller en främmande stats datatrafik kommer i fråga endast i sådana fall, där i det datatrafikflöde som styrs till underrättelsesystemet inte av misstag kan följa med sådan datatrafik som åtnjuter skydd för hemligheten i fråga om förtrolig kommunikation. I praktiken förutsätter detta att den del av ett kommunikationsnät som domstolens tillstånd gäller och som sökbegreppen riktas mot är reserverad för statlig datatrafik. Användningen av ett undantag som gäller en främmande stats datatrafik blir därmed i praktiken snäv.

En förutsättning för underrättelseinhämtning som riktas mot en statlig aktörs datatrafik ska vara det resultatkrav som är en allmän förutsättning för underrättelseinhämtning. Befogenheten ska kunna utövas, om detta med fog kan antas vara av betydelse med tanke på ett underrättelseuppdrag.

Underrättelseinhämtning som avser datatrafik i enlighet med 1 mom. ska det vara möjligt att använda vid underrättelseinhämtning från en statlig aktörs datatrafik. Underrättelseinhämtning som avser datatrafik ska omfatta insamlandet, lagrandet och behandlingen av datatrafik i syfte att inhämta underrättelser.

Vid underrättelseinhämtning som gäller en statlig aktörs datatrafik ska i den första fasen i den datatrafik som styrts till Försvarsmaktens underrättelsetjänst sökas efter data som är väsentliga med tanke på ett underrättelseuppdrag i den del av ett kommunikationsnät som fastställs i det tillstånd som domstolen har beviljat. Bestämmelser om domstolens tillstånd finns nedan.

I situationer enligt 1 mom. ska insamlandet göras med hjälp av automatisk databehandling, som ska basera sig på sökbegrepp. Genom detta görs det en åtskillnad till övriga metoder för underrättelseinhämtning som riktas mot datatrafik i kommunikationsnätet, framför allt till teleavlyssning och teleövervakning, om vilka föreskrivs tidigare i detta kapitel, samt till teleavlyssning och teleövervakning om vilka föreskrivs i polis- och tvångsmedelslagen. Teleavlyssning inriktas exakt på en sådan teleterminalutrustning eller teleadress, vars identifieringsuppgifter är klara när underrättelseinhämtningen inleds eller på en person som man känner till på förhand. I den underrättelseinhämtning som avser datatrafik är det inte fråga om att inhämta information genom inriktning på en på förhand identifierad teleterminalutrustning eller teleadress, utan om att filtrera ut datatrafik i en viss del av kommunikationsnätet genom automatiserade datatekniska metoder för att hitta data som anknyter till ett visst underrättelseuppdrag. I den underrättelseinhämtning som riktar sig mot en statlig aktörs datatrafik ska insamlandet i praktiken genomföras så att en viss del av kommunikationsnätet identifieras där den statliga aktörens datatrafik rör sig och vid behov ska datatrafiken jämföras med kriterier som ställs på förhand och som kallas sökbegrepp. Ett syfte med den underrättelseinhämtning som avser datatrafik ska också vara att identifiera enskilda teleterminalutrustningar och teleadresser för att möjliggöra teleavlyssning eller teleövervakning.

Enligt den sista meningen i momentet ska inhämtningen av information om en statlig aktörs datatrafik grunda sig på användningen av sökbegrepp. Sökbegreppen beskrivs närmare i detaljmotiveringen till 67 §.

Insamlande som grundar sig på sökbegrepp ska riktas bara mot datatrafik som rör sig i en viss del av kommunikationsnätet. Denna kommunikationsnätsdel ska ha definierats i domstolens

tillståndsbeslut, eller i exceptionella situationer, i ett tillfälligt beslut som Huvudstabens underrättelsechef har fattat i en brådskande situation. Det datatrafikflöde som går i kommunikationsnätsdelen i fråga ska styras så att det också går via underrättelsesystemet, varvid underrättelsesystemet samlar in och lagrar datatrafik som stämmer överens med sökbegrepp som på förhand har förts in i systemet. Insamlandet och lagrandet ska ske genom automatisk databehandling, vilket gör att ingen fysisk person ser den datatrafik som går genom underrättelsesystemet. Endast den trafik som motsvarar sökbegreppen lagras i systemet så att militärunderrättelsemyndighetens tjänsteman kan behandla den.

Försvarsmaktens underrättelsetjänst ska inte ha rätt eller möjlighet att lagra annan trafik än den som motsvarar sökbegreppen enligt det tillstånd som domstolen har beviljat. Militärunderrättelsemyndigheten ska inte heller i efterskott ha möjlighet att på nytt ta upp eller granska data som inte har motsvarat villkoren enligt det beslut som domstolen har beviljat. En myndighet som använder sig av underrättelseinhämtning som avser datatrafik ska inte i någon som helst situation få tillträde till annan än den datatrafik som motsvarar sökbegreppen.

Försvarsmaktens primära uppgift enligt 2 § 1 mom. 1 punkten i lagen om försvarsmakten är det militära försvaret av Finland. Militära hot orsakas mest centralt av främmande stater. Enligt paragrafen ska underrättelseinhämtning som avser datatrafik kunna användas för underrättelseinhämtning från en främmande stats kommunikation. Från en främmande stats kommunikation kan man få väsentlig information om den främmande statens planer och handlingsförmåga, vilka direkt påverkar det hot som riktas mot Finland och beredskapen inför det. Genom en effektiv underrättelseinhämtning kan militärunderrättelsemyndigheterna utforma en förvarning om ett militärt hot som riktas mot landet och hur man ska förbereda sig på det.

Enligt 2 mom. ska Försvarsmaktens underrättelsetjänst ha möjlighet att automatiskt och manuellt behandla den information som erhållits med automatisk databehandling. På detta stadium ska en tjänsteman vid Försvarsmaktens underrättelsetjänst få möjlighet att behandla den insamlade datakommunikationen och meddelandenas innehåll för att hitta de meddelanden som är väsentliga med tanke på underrättelseuppdraget och för att analysera dem.

I analyseringsfasen ska med automatisk behandling avses sådan analysering av en insamlad uppgift som genomförs med automatisk databehandling, dvs. med ett tekniskt informationssystem. För detta kan användas t.ex. en algoritm som utvecklats för analysering. Största delen av analyseringen av den insamlade informationen ska i praktiken göras automatiskt. Syftet med den automatiska behandlingen ska vara t.ex. att på den insamlade informationen inrikta sådana sökningar med hjälp av vilka mängden information som ska bli föremål för manuell behandling kan minskas. Den analysering och de sökningar som ska göras med hjälp av ett informationssystem ska kunna gälla såväl förmedlingsuppgifter och andra styruppgifter som ingår i den insamlade informationen som också innehåll av betydelse i sådan information.

Insamlad och lagrad information ska också kunna behandlas med sinnesförnimmelser på åtgärd av en fysisk person. Eftersom man i en dylik behandling liksom också i den automatiska behandlingen ovan ska få reda ut ett meddelandes förmedlingsuppgifter och innehåll, ska i behandlingen med sinnesförnimmelser ingå t.ex. att en tjänsteman som är anställd vid Försvarsmaktens underrättelsetjänst läser textinnehållet i det meddelande som behandlas, granskar bildbilagor till det, lyssnar på ljud eller matar in meddelandets innehåll i den programvara som avsändaren har avsett meddelandet för, för att följa med programvarans prestation.

Om det medan ett meddelande behandlas, framgår att den information som är föremål för behandlingen inte kommer att ge väsentlig information med tanke på ett underrättelseuppdrag el-

ler om man inte annars skulle få inhämta information från meddelandet, ska det utan dröjsmål utplånas utgående från de bestämmelser som gäller utplåning.

För aktörer som är etablerade på finskt territorium ställs ingen skyldighet att installera s.k. bakdörrar till programvaror som använder kryptering och aktörerna åläggs inte heller att överlåta krypteringsnycklar eller annars begränsa användningen av krypteringsteknik.

I paragrafens 3 mom. ska det föreskrivas om ett uttryckligt förbud mot att i den underrättelseinhämtning som inriktas mot en statlig aktörs datatrafik använda uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland. De hot som orsakas av föremålen för militär underrättelseinhämtning enligt paragrafen kommer från platser utanför Finlands gränser. De som orsakar hot är dessutom stora organiserade aktörer.

**66 §.** *Beslut om underrättelseinhämtning som avser en statlig aktörs datatrafik.* Staten och andra offentliga sammanslutningar åtnjuter inte skydd för de grundläggande fri- och rättigheterna (RP 309/1993 rd och GrUU 9/2015 rd). Eftersom t.ex. en främmande stats militärorganisations kommunikation inte åtnjuter skyddet för hemligheten i fråga om ett förtroligt meddelande, ska man kunna besluta om att samla in, lagra och behandla en statlig aktörs kommunikation med lindrigare förutsättningar än när det är fråga om insamlande, lagring och behandling av en annan aktörs kommunikation.

Enligt paragrafens 1 mom. ska Helsingfors tingsrätt på yrkande av Huvudstabens underrättelsechef besluta om rätten att inrikta underrättelseinhämtning på datatrafiken hos en sådan statlig aktör som avses i 65 §.

I momentets två sista meningar ska det föreskrivas om en brådskande situation där ärendet inte tål uppskov. Beslutet ska kunna fattas av Huvudstabens underrättelsechef till dess domstolen har avgjort yrkandet om beviljande av tillstånd. När en statlig aktörs kommunikation samlas in, lagras och behandlas kan det komma situationer där insamlandet, lagrandet och behandlingen av den statliga aktörens kommunikation måste kunna inledas omedelbart till följd av information som man erhållit överraskande eller en snabbt föränderlig verksamhetsomgivning. Yrkandet ska föras till domstolen inom 24 timmar från det utövandet av befogenheten inleddes.

Tillstånd ska i enlighet med 2 mom. kunna ges för högst sex månader åt gången.

I 3 mom. ska det föreskrivas om uppgifterna i tillståndsansökan. Enligt 1 punkten i momentet ska i tillståndsansökan nämnas det underrättelseuppdrag för vilket informationsinhämtning ska riktas mot en statlig aktörs datatrafik. I beskrivningen av underrättelseuppdraget ska en större helhet specificeras för vilken informationsinhämtning från en viss statlig aktör behövs. Underrättelseuppdraget har beskrivits ovan i motiveringen till 9 §.

Enligt 2 punkten ska i ansökan anges de sökbegrepp eller kategorier av sökbegrepp utgående från vilka kommunikation ska samlas in, lagras och behandlas. Utgående från sökbegrepp eller kategorier av sökbegrepp ska information som är väsentlig med tanke på ett underrättelseuppdrag letas efter bland en stor mängd datatrafik. För att den underrättelseinhämtning som avser datatrafik ska vara tillräckligt inriktad, ska de sökbegrepp som används vara tillräckligt exakta så att information som är onödig med tanke på underrättelseuppdraget inte av misstag kommer med i den manuella behandlingen av datatrafiken.

Sökbegreppen ska beskriva föremålet för informationsinhämtningen. De statliga aktörerna är stora organisationer. Till följd av det som sägs ovan sammanhänger ett enormt antal förmedlingsuppgifter med föremålet för ett underrättelseuppdrag, utgående från vilka information ska inhämtas om föremålet för underrättelseuppdraget. I de sökbegrepp som ska presenteras i tillståndsansökan ska ingå de grupper av sökbegrepp utgående från vilka den underrättelseinhämtning som avser datatrafik ska inriktas. Grupperna ska innehålla mera exakta förmedlingsuppgifter gällande en viss organisation som är väsentlig med tanke på underrättelseuppdraget, såsom en organisation som utvecklar ett visst nytt vapensystem.

Enligt 2 punkten ska de valda sökbegreppen eller kategorierna av sökbegrepp också motiveras i yrkandet. I motiveringarna ska det anföras mera exakt för vilket ändamål och hur kommunikation som är väsentlig med tanke på ett underrättelseuppdrag med de valda sökbegreppen eller kategorierna av sökbegrepp ska få samlas in från en kommunikationsnätsdel som avses i 3 punkten och lagras.

Den som framför yrkandet ska ha en accentuerad skyldighet att se till att de sökbegrepp och kategorier av sökbegrepp som anförts i yrkandet inriktas på datatrafiken hos den part från vilken man med tanke på ett underrättelseuppdrag ska inhämta information. I samband med behandlingen av yrkandet ska domstolen genom att använda sin rätt till utfrågning försäkra sig om att sökbegreppen och kategorierna av sökbegrepp är så tillräckliga att den underrättelseinhämtning som avser datatrafik inriktas på just det objekt som avses i yrkandet.

Eftersom en statlig aktör inte åtnjuter skyddet för hemligheten i fråga om ett förtroligt meddelande, ska som sökbegrepp också kunna användas uppgifter som beskriver innehållet i ett meddelande. I underrättelseinhämtning som riktas mot en statlig aktörs datatrafik kan man emellertid behöva använda sökbegrepp som riktas mot ett meddelandes innehåll till följd av den stora mängden datatrafik eller för att man redan på detta stadium ska få bortsållat sådan kommunikation i den statliga aktörens datatrafik som till innehållet omfattas av skyddet för hemligheten i fråga om ett förtroligt meddelande.

Enligt 3 punkten ska i ansökan anmälas de delar av kommunikationsnätet som överskrider Finlands gräns, såsom trådfibrer, där kommunikation ska samlas in och lagras. Till exempel genom att underrättelseinhämtning som avser datatrafik inriktas på enskilda fibrer ställs en betydande del av den datatrafik som överskrider Finlands gränser utanför informationsinhämtningen, vilket för sin del också effektiverar och inriktar den underrättelseinhämtning som avser datatrafik på korrekt sätt. I ansökan ska det motiveras varför en statlig aktörs kommunikation som är väsentlig med tanke på ett underrättelseuppdrag kan samlas in och lagras från just den del av kommunikationsnätet som valts.

Den som anför ett yrkande ska ha en accentuerad skyldighet att motivera varför en statlig aktörs datatrafik flödar just i en viss del av kommunikationsnätet. Domstolen ska genom att använda sig av sin utfrågningsrätt kunna försäkra sig om att datatrafik från och till den statliga aktören flödar i just den kommunikationsnätsdel som anförs i yrkandet.

Enligt 4 punkten ska det i tillståndsansökan meddelas hur länge tillståndet är giltigt med angivande av klockslag. Såsom i fråga om övriga metoder för underrättelseinhämtning, ska den inhämtade informationen hela tiden bedömas, och inhämtandet ska avbrytas när information som är väsentlig för ett underrättelseuppdrag har inhämtats. Vidare kan i fråga om ett tillstånds giltighet hänvisas till det som konstateras i detaljmotiveringen till 20 §.

Enligt 5 punkten ska för underrättelseinhämtning som avser datatrafik i enlighet med tillståndet utnämnas en tjänsteman som är särskilt förtrogen med användningen av Försvarsmaktens underrättelsetjänsts metoder för underrättelseinhämtning för att leda och övervaka genomförandet av underrättelseinhämtningen.

Enligt 6 punkten ska andra villkor och begränsningar som eventuellt ställs för den underrättelseinhämtning som avser en statlig aktörs datatrafik nämnas.

**67 §.** *Underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer*. I paragrafen ska det föreskrivas om underrättelseinhämtning som avser datatrafik hos någon annan än en statlig aktör samt om förutsättningarna för utövandet av befogenheten. Utöver de förutsättningar om vilka föreskrivs i paragrafen ska när förutsättningarna för att utöva befogenheten övervägs också underrättelseverksamhetens allmänna principer beaktas.

Med andra än statliga aktörer ska avses föremål för ett underrättelseuppdrag som inte kan anses vara en främmande stat eller en med en sådan jämställbar aktör. När en aktörs ställning bedöms ska uppmärksamhet ägnas aktören, aktörens organisation, de resurser som aktören har till sitt förfogande och framför allt, huruvida aktören anknyter till ett föremål för militär underrättelseinhämtning.

Sådana som avses ovan och som är andra än statliga aktörer kan vara t.ex. företag som utvecklar vapenteknik och andra än militära organisationer som stöder truppförband. Den militära underrättelseinhämtningen kan vidare få väsentlig information också från många organisationer som anknyter till vapenindustrin.

Vidare ska underrättelseinhämtning som riktas mot datatrafiken hos någon annan än en statlig aktör komma i fråga i situationer där man på grund av internets art inte med tillräcklig sannolikhet kan på förhand anföra att datatrafik som flödar i en viss del av kommunikationsnätet endast är en statlig aktörs datatrafik. En sådan situation kan komma i fråga t.ex. när en statlig aktör under en viss tid använder vanliga mobiltelefoner i ett allmänt kommunikationsnät i ett område som har identifierats på förhand.

Till skillnad från det som föreskrivs i 65 § om underrättelseinhämtning som inriktas på en statlig aktörs datatrafik, ska i de situationer som avses i denna paragraf ställas strängare krav på underrättelseinhämtning som avser datatrafik. Underrättelseinhämtningen ska tekniskt göras på samma sätt utifrån sökbegrepp som det som beskrivs i motiveringarna till 65 §, men med strängare krav.

Enligt 1 mom. ska datatrafik hos andra än statliga aktörer, vilken är väsentlig med avseende på ett underrättelseuppdrag, kunna inhämtas om den underrättelseinhämtning som riktas mot datatrafiken hos någon annan än en statlig aktör kan antas vara nödvändig för att inhämta information med avseende på ett underrättelseuppdrag.

För underrättelseinhämtning som avser datatrafik ska till denna del ställas ett strängare krav än för de föreslagna metoder för underrättelseinhämtning som ska ingripa i skyddet för hemligheten i fråga om ett förtroligt meddelande eller den underrättelse som avses i 65 § och inriktas på en statlig aktörs datatrafik. Skälet till detta är Europeiska människorättsdomstolens avgörande i fallet Szabo & Vissy v. Ungern, enligt vilket förutsättningen ”nödvändigt i ett demokratiskt samhälle” enligt artikel 8 i konventionen om mänskliga rättigheter i samband med övervakningsteknik som representerar spetsen av utvecklingen inom underrättelseinhämtning som avser datatrafik ska tolkas så att den förutsätter ”ovillkorlig nödvändighet” (strict neces-

sity) i två sammanhang. För det första bör användningen av metoden på allmän nivå vara ovillkorligt nödvändig för att skydda demokratiska institutioner. För det andra bör användningen av metoden i samband med en enskild underrättelseinsats vara ovillkorligt nödvändig för att man ska få vital information.

Den nödvändighetsförutsättning som föreslås för användningen av underrättelseinhämtning som avser datatrafik ska användas i sista hand, dvs. i praktiken om informationsinhämtning med någon annan metod än underrättelseinhämtning som avser datatrafik inte är möjlig eller t.ex. skulle kräva väsentligt mera resurser eller fördröja informationsinhämtningen oskäligt mycket. Med iakttagande av de kriterier som har ställts för bedömning av nödvändigheten i den regeringsproposition som gällde revidering av tvångsmedelslagen (RP 222/2010 rd, s. 326) förutsätts dock ingen utredning av den faktiska användningen av andra metoder för underrättelseinhämtning eller försök med sådana, eftersom i så fall skulle man bli tvungen att vidta dyra och onödiga åtgärder som skulle drabba integritetsskyddet. Nödvändigheten kan grundas på en helhetsbedömning av att andra metoder skulle vara t.ex. resultatlösa eller inte lämpa sig för informationsinhämtningen utan att man konkret skulle ha försökt använda dem. Det är till exempel inte nödvändigtvis möjligt att följa med meddelandetrafiken till och från en aktör som befinner sig utanför Finlands gränser med andra metoder för underrättelseinhämtning, eftersom den kommunikation som är föremål för underrättelseinhämtningen inte kan följas med tillräckligt obemärkt eller kommunikationen inte kan samlas in och lagras i tillräckligt snabb takt.

Fastän inhämtandet av information i sig vore möjligt med användning av en annan metod för underrättelseinhämtning, är det inte nödvändigtvis motiverat att använda en annan metod för underrättelseinhämtning till följd av de finansiella resurser eller personalresurser som står till den militära underrättelseinhämtningens förfogande. Följaktligen förutsätter tillämpningen av bestämmelsen en jämförelse mellan å ena sidan de metoder för underrättelseinhämtning om vilka föreslås bli föreskrivet i andra kapitel, i synnerhet teleavlyssning och teleövervakning, och å andra sidan den underrättelseinhämtning som avser datatrafik. Eftersom användningen av teleavlyssning och teleövervakning i regel kan inriktas mera exakt än användningen av underrättelseinhämtning som avser datatrafik, innehåller användningen av teleavlyssning och teleövervakning också en mindre möjlighet att utomståendes kommunikation omfattas av underrättelseinhämtningen. Således, om det i ett enskilt fall inte är omöjligt eller mycket svårt att använda teleavlyssning eller teleövervakning, ska de användas som primära metoder i relation till den underrättelseinhämtning som avser datatrafik.

Vidare kan det vara särskilt svårt för den som genomför en underrättelseinsats att inhämta information med andra metoder. Det är betydligt tryggare att genomföra en underrättelseinsats hemifrån än att genomföra den på en främmande stats territorium.

Till nödvändighetsförutsättningen ska på bestämmelsenivå inte fogas ett krav på att den information som erhålls genom underrättelseinhämtning som avser datatrafik ska vara synnerligen viktig. Detta beror på att det i underrättelseverksamhet är svårare att bedöma om information är synnerligen viktig än t.ex. vid brottsbekämpning, där en konkret gärning ska förhindras, avslöjas eller redas ut.

I underrättelseinhämtning och i synnerhet i den underrättelseinhämtning som avser datatrafik är det emellertid inte fråga om endast att avvärja omedelbara faror, utan också om långvarigare informationsinhämtning om verksamhet som allvarligt äventyrar den nationella säkerheten. Underrättelseinhämtning som avser datatrafik kan vara nödvändig t.ex. för att inhämta sådan information som i följande fas möjliggör användningen av någon av de metoder för under-

rättelseinhämtning som avses i detta kapitel, men som inte ännu ensam kan anses vara nödvändig för att inhämta information som gör det möjligt att avvärja ett hot. Den militära underrättelseinhämtningen ska vara en helhet bestående av flera metoder för underrättelseinhämtning som kompletterar varandra. Inom ramen för den är det ytterst svårt att på förhand bedöma och visa vilken betydelse information som erhålls med var och en enskild metod har med tanke på den övergripande uppfattningen om den verksamhet som är föremål för informationsinhämtningen.

Enligt den sista meningen i momentet ska underrättelseinhämtning som avser datatrafiken hos någon annan än en statlig aktör grunda sig på användning av sökbegrepp. Enligt principen om minsta olägenhet, som har föreskrivits som en allmän princip som styr underrättelseverksamheten, ska kombinationer av sökbegrepp och kategorier av sökbegrepp vara sådana att de så exakt som möjligt avgränsar datatrafiken hos den part som är föremål för underrättelseinhämtning som avser datatrafik och inte är en statlig aktör. Vidare ska principen om ändamålsbundenhet styra underrättelsemyndigheterna att utarbeta sökbegreppskombinationer och sökbegreppskategorier så att befogenheten kan användas för endast det syfte som den är avsedd för. Proportionalitetsprincipen ska också styra underrättelsemyndigheterna vid utarbetandet av sökbegrepp.

Bestämmelser om skyldigheten att anföra sökbegrepp eller kategorier av sökbegrepp samt motiveringar till dem i domstolsbehandlingen ska ingå i 68 § 3 mom. 4 punkten.

Insamlande och lagrande som riktas mot datatrafiken hos någon annan än en statlig aktör ska enligt 2 mom. inte få göras utgående från uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland. Föremål för den militära underrättelseinhämtningen ska inte vara enskilda personer som vistas i Finland. Insamlandet och lagrandet av kommunikationen hos andra än statliga aktörer inriktas på stora aktörer som är verksamma utanför Finlands gränser. Uppgifter om en teleterminalutrustning eller teleadress som innehas eller används av en person som vistas i Finland kan vid behov inhämtas med de befogenheter som avses i 4 kapitlet. Till exempel informationsinhämtning som riktas mot en mobiltelefon i ett finskt nät kan genomföras med de metoder för underrättelseinhämtning om vilka det föreslås att ska föreskrivas i 4 kapitlet, varvid konsekvenserna för utomståendes datakommunikation kan minimeras.

I 3 momentet ska det föreskrivas om ett uttryckligt förbud mot att genomföra underrättelseinhämtning som avser datatrafik utifrån innehållet i ett meddelande. Insamlande och lagrande av datatrafik ska endast få ske utgående från sökbegrepp eller kategorier av sökbegrepp som stämmer överens med tillståndet. Dessa ska inriktas på andra uppgifter i anknytning till kommunikationen än uppgifter som ingår i meddelandets innehåll.

Ett undantag till det som sägs ovan ska dock vara uppgifter som beskriver innehållet i ett sabotageprogram och dess egenskaper. Den huvudsakliga uppgiften för underrättelseverksamheten är inte att förbättra datasäkerheten, men i samband med underrättelseinhämtning som avser datatrafik ska man utan att äventyra integritetsskyddet i samband med ett underrättelseuppdrag kunna få information om ett sabotageprogram som rör sig i datanäten. Det är i allmänhet mest effektivt att identifiera tekniska nätattacker så nära ett system, som potentiellt kan vara mål för en attack, som möjligt och på åtgärd av systemets egna underhållsansvariga. Det finns emellertid situationer där de eventuella målen är många eller underhållet av de potentiella målsystemen har lagts ut på entreprenad till någon sådan kostnadsfri part som gör att det inte är möjligt att överlåta detaljerad information om avvärjningsindikatorer utan att den nationella säkerheten äventyras. Då ska information om attacker eller förberedande åtgärder kunna inhäm-

tas genom underrättelseinhämtning som avser datatrafik. De sabotageprogram som avses i momentet är högt utvecklade och bakom utvecklandet av dem finns ofta en statlig aktör och bakom verksamheten ligger statliga intressen. Utöver spionerі som riktar sig mot finska staten förekommer också strävanden efter intressen som anknyter till industrin och näringslivet. De finska organisationernas datasäkerhet ska fortfarande organisationerna själva svara för. Information om sabotageprogram ska kunna ges till samhällets olika aktörer på det sätt som föreskrivs i 77 §.

Efter ett inträffat datasäkerhetsintrång kan man försöka identifiera en avvikelse utifrån ett trafikflöde av mängd egenskaper som orsakats av ett sabotageprogram eller ett skadligt kommando. Däremot är det ofta inte möjligt att göra avvärjandet på förhand med stöd av enbart rubrikuppgifter eller särdrag i trafikflödet i datatrafiken, eftersom den datatrafik som föregår intrånget strävar efter att maskera sig till sedvanlig kommunikation. Därför ska det föreskrivas om ett undantag som gör det möjligt att söka i innehållet i trafik som innehåller ett skadligt datorprogram eller kommando.

Med skadlighet avses här äventyrande av den tekniska datasäkerheten, dvs. ett datorprogram eller kommando som strävar efter att stjäla information, ändra information utan att ha rätt till det eller skada målsystemets verksamhet. Som målsystem ska anses vilket som helst digitalt system, också själva nätet, dvs. de nätanordningar som styr datatrafiken samt de anordningar som styr processerna i den reella världen. Eftersom sökbegrepp inte ska vara ett ord i ett naturligt språk, utan någon teknisk teckensträng, ska kravet på avgränsning av vilken datatrafik som blir utsatt för automatisk jämförelse inte vara lika strängt som vid underrättelseinhämtning som avses datatrafiken i övrigt.

I dessa situationer är det fråga om t.ex. ett sabotageprogram, i fråga om vilket det utgående från på förhand erhållen information har identifierats att det tränger in i datasystem via stora IKT-tjänstetillhandahållares system. I en sådan situation kan det vara fråga om ett hot, som allvarligt äventyrar också finska myndigheters verksamhetsförmåga, om motsvarande situation realiseras i datasystemen hos de IKT-tjänstetillhandahållare som finska myndigheter använder. I detta fall inriktas informationsinhämtningen på huruvida sabotageprogrammet i fråga kan upptäckas i de finska datanäten. Den inhämtade informationen är väsentlig för att det finska samhället ska kunna skydda sig samt med tanke på en bedömning av situationen som helhet i fråga om säkerheten.

I 4 momentet ska det föreskrivas om möjligheten att automatiskt och manuellt behandla den datatrafik som avses i 1 mom. och som har inhämtats automatiserat. Vid den manuella behandlingen ska väsentliga uppgifter med tanke på ett underrättelseuppdrag inhämtas ur innehållet i meddelandena.

Vid automatisk behandling och sådan behandling som grundar sig på sinnesförnimmelser ska ett meddelandes förmedlingsuppgifter och lokaliseringsuppgifter samt meddelandets innehåll få redas ut. Genom att nämna meddelandets innehåll tar man officiellt upp det att alla sådana uppgifter som åtnjuter skydd för hemligheten i fråga om ett förtroligt meddelande kan bli föremål för utredning. Utöver de ovan nämnda uppgifterna som åtnjuter skydd för hemligheten i fråga om ett förtroligt meddelande får vid automatisk och manuell behandling utan särskilt omnämnande i bestämmelserna utredas också sådana uppgifter i anknytning till styrningen av datatrafiken, vilka inte omfattas av skyddet för hemligheten i fråga om ett förtroligt meddelande.

För aktörer som är etablerade på finskt territorium ställs ingen skyldighet att installera s.k. bakdörrar till programvaror som använder kryptering och aktörerna åläggs inte heller att överlåta krypteringsnycklar.

**68 §.** *Beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer.* Enligt 1 mom. ska Huvudstabens underrättelsechef anföra ett yrkande hos domstolen. I de två sista meningarna i momentet ska det föreskrivas om beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer i en brådskande situation. I dessa situationer ska beslutet fattas av Huvudstabens underrättelsechef.

Vid underrättelseinhämtning som avser datatrafik kan det uppkomma sådana situationer där man snabbt måste reagera t.ex. av den anledningen att de sökbegrepp som anknyter till föremålet för ett underrättelseuppdrag eller andra väsentliga uppgifter som anknyter till inriktningen, såsom dirigeringsuppgifter, ändras. Vidare kan det medan underrättelseinhämtning som avser datatrafik pågår uppkomma situationer, där man utifrån en ny erhållen uppgift kan få väsentliga uppgifter som anknyter till underrättelseuppdraget, men gällande tillstånd inte täcker sådan informationsinhämtning.

Efter att Huvudstabens underrättelsechef har fattat beslut ska ärendet föras till domstol så snart det är möjligt, dock senast inom 24 timmar från det att den brådskande underrättelseinhämtning som avser datatrafik började användas. När domstolen har bedömt förutsättningarna för beslutet, ska tillstånd kunna meddelas eller också ska domstolen kunna avslå yrkandet. Bestämmelser om avslutande av användningen av en metod för underrättelseinhämtning som har inletts i en brådskande situation finns nedan.

Ett förfarande i en brådskande situation kan bedömas vara ytterst exceptionellt på grund av att domstolen har jour. En sådan situation kan komma i fråga, om man av ett eller annat skäl inte kan ordna ett domstolsförfarande och tillträde till domstolen är förhindrat. Vidare kan det i en situation vara fråga om t.ex. att reda ut var en finländare, som har tagits som gisslan i ett krishanteringsområde, befinner sig och situationen bedöms vara så kritisk att underrättelseinhämtning som avser datatrafik måste kunna användas genast.

Enligt 2 mom. ska tillstånd få beviljas för högst sex månader åt gången.

I 3 mom. ska det föreskrivas om den information som ska anges i yrkandet och beslutet.

Enligt 1 punkten i momentet ska i tillståndsansökan nämnas det underrättelseuppdrag för vilket informationsinhämtning ska riktas mot datatrafiken hos någon annan än en statlig aktör. I beskrivningen av underrättelseuppdraget ska en större helhet specificeras för vilken informationsinhämtning från datatrafiken hos någon annan än en statlig aktör behövs.

Enligt 2 punkten ska i yrkandet och beslutet nämnas de fakta gällande föremålet, vilka ger anledning att anta att någon annan än en statlig aktör anknyter till underrättelseuppdraget. Militärunderrättelsemyndigheten ska således i det yrkande den anför hos domstolen klargöra tillräckligt exakt arten av den konkreta verksamhet som man har för avsikt att inhämta information om med den underrättelseinhämtning som avser datatrafik. Den information som ska ges i yrkandet ska kunna gälla t.ex. hur man fått kännedom om verksamheten, hur verksamheten hittills har visat sig, hur det antas att verksamheten kommer att utvecklas, vilken part eller vilka personer som står bakom verksamheten och till vilka delar och på vilket sätt verksamheten anknyter till underrättelseuppdraget. För att tillstånd ska beviljas ska det förutsättas att domstolen utifrån de fakta som presenteras för den blir övertygad om att den konkreta verk-

samhet som är föremål för yrkandet anknyter till underrättelseuppdraget. Den som anför ett yrkande ska därmed kunna påvisa att konkret verksamhet, utifrån de fakta man känner till om den, i sista hand svarar mot det eller de föremål för militär underrättelseinhämtning som ska specificeras i yrkandet eller beslutet enligt 1 punkten.

Enligt 3 punkten ska i yrkandet och beslutet nämnas de fakta som förutsättningarna för användning av underrättelseinhämtning som avser datatrafik grundar sig på. Försvarsmaktens underrättelsetjänst ska i sitt yrkande redogöra för de fakta utgående från vilka man med underrättelseinhämtning som avser datatrafik överhuvudtaget kan antas få uppgifter om den för underrättelseuppdraget väsentliga aktör som yrkandet gäller. Vidare ska i yrkandet enligt punkten redogöras för att den nödvändighet som ställts som förutsättning uppfylls. Såväl i yrkandet som i domstolens beslut ska det därmed redogöras för varför de uppgifter som man har för avsikt att inhämta med underrättelseinhämtning som avser datatrafik i fallet i fråga inte kan inhämtas på något annat sätt, eller varför inhämtandet av dem på något annat sätt skulle vara väsentligt svårare eller farligare. I yrkandet ska det presenteras en bedömning av varför just informationsinhämtning genom underrättelseinhämtning som avser datatrafik i situationen i fråga är en bättre metod än övriga metoder för underrättelseinhämtning när det gäller att inhämta uppgifter som är föremål för ett underrättelseuppdrag.

Enligt 4 punkten ska i yrkandet och beslutet anges de sökbegrepp eller kategorier av sökbegrepp utifrån vilka datatrafik ska inhämtas samt motiveringar till dem. Utgående från sökbegrepp eller kategorier av sökbegrepp ska information som är väsentlig med tanke på ett underrättelseuppdrag letas efter bland ett stort flöde av datatrafik i en viss del av kommunikationsnätet. För att den underrättelseinhämtning som avser datatrafik ska vara tillräckligt inriktad, ska de sökbegrepp som används vara tillräckligt exakta för att information som är onödig med tanke på underrättelseuppdraget inte ska komma med i behandlingen av kommunikationen. De allmänna principerna i lagen ska gälla underrättelsemyndigheterna också då sökbegrepp och kategorier av sökbegrepp utarbetas.

Sökbegreppen ska beskriva föremålet för informationsinhämtningen och rikta in sig på den del av föremålets kommunikation som inte utgör kommunikationens innehåll. Sådana uppgifter är t.ex. meddelandets förmedlingsuppgifter och andra tekniska uppgifter. Sökbegrepp kan vara t.ex. AS-nummer, IP-adressområden samt domännamn.

Enligt huvudregeln får ett sökbegrepp inte beskriva innehållet i ett meddelande, vilket gör att som sökbegrepp inte får tas formuleringar som används av de personer som sänder meddelanden. Begreppens innehåll och styrinformation förutsätter i internet en mera omfattande definition och förklaring än i de gamla telefonnäten, eftersom gränsen mellan innehåll och rubrikinformation kan variera i hög grad beroende på i vilket skikt av OSI-modellen, som beskriver verksamheten i nättrafiken, man granskar saken. Det finns två tolkningar i saken. I bådadera skiljer sig konsekvenserna för de grundläggande fri- och rättigheterna av tillämpningen av dem betydligt från varandra.

Om innehållet skiljs åt från styrinformationen utgående från transportskiktet, är styrinformationen endast den information, med vilken meddelandet styrs i nätet. Granskat i transportskiktet kan sökbegrepp således vara endast anordningarnas nätadress, eftersom t.ex. e-postadressen transporteras inne i datatrafikpaketets nyttolast i transportskiktet. Underrättelseinhämtningen ska i detta fall inte kunna begränsas genom ett sökbegrepp t.ex. till en enskild e-postadress (t.ex. xx.xxx@epost.com). All e-posttrafik i servern gmail.com skulle man bli tvungen att införliva i en manuell innehållsanalys utförd av en tjänsteman. Men sökning ur

transportskiktet skulle å andra sidan vara synnerligen rätlinjig. Inget datatrafikpakets nyttolast öppnas, utan insamlandet och lagrandet ska ske utgående från rubrikfält.

Om igen innehållet skiljs åt från styrinformationen utgående från applikationsskiktet, omfattar styrinformationen också den information utgående från vilken ett meddelande styrs exakt till rätt mottagare i den mottagande anordningens kommunikationsprogramvara. Granskat i applikationsskiktet kan man därmed i datatrafiken mellan epostservrar utanför och i Finland genom sökbegrepp sålla fram för innehållsanalys endast den datatrafik som gäller en adress (xx.xxx@epost.com), annan trafik i servern ska lämnas utanför insamlandet och lagrandet. Å andra sidan förutsätter en analys av rubrikinformationen i applikationsskiktet att den nyttolast som valts ut i paketen i datatrafikflödets transportskikt måste öppnas med en teknisk analysator för att applikationsskiktets rubrikinformation ska kunna jämföras med sökbegreppen.

Den tolkning av skillnaden mellan innehåll och tekniska data som använts vid underrättelseinhämtning som avser datatrafik står närmare tolkningen av OSI-modellens applikationsskikt än tolkningen av transportskiktet. Då kan sökandet efter det material som kommer till innehållsanalys inriktas betydligt exaktare, varvid konsekvenserna för de grundläggande fri- och rättigheterna av underrättelseinhämtningen blir mindre.

Gränsen är dock inte till sin art rätlinjigt datateknisk, utan som rättesnöre för tolkningen bör tas syftet med den teckensträng som valts som sökbegrepp i datatrafikflödet: Förekommer den i dataflödet för att styra meddelandeinnehållet eller är den avsedd som ett semantiskt budskapsinnehåll från avsändaren till mottagaren. Gränsen kan åskådliggöras genom det fält i ett epostmeddelande där det står: ”Ämne”. Ett epostmeddelandes Ämnesfält visas i tillämpningarna bland rubrikinformationen. Om avsändaren har avsett det som ett budskap till den person som är meddelandets mottagare, kan det inte anses som styrinformation, utan som ett semantiskt innehåll. De sökbegrepp som ska användas i underrättelseinhämtning som avser datatrafik ska bestå av alla sådana uppgifter som används för att styra eller dokumentera ett meddelandes gång i meddelandesystemet, medan igen innehåll ska vara all sådan information som avsändaren har avsett att ge mottagaren. Därmed kommer adresser i fråga, såväl användaridentifikationer i de sociala mediernas tjänster som också teleadresser. Ett sökbegrepp ska också kunna vara konstruerat så att det utgörs av en styrinformationsmängd, t.ex. en kombination av IP-adress, målport och identifikator till ett transportskikt.

Med föremålet för ett underrättelseuppdrag kan sammanhänga ett stort antal förmedlingsuppgifter, utgående från vilka datatrafik samlas in från föremålet för underrättelseuppdraget.

I ett yrkande ska också kunna anföras kategorier av sökbegrepp, utgående från vilka avskiljandet av datatrafik ska ske. Med kategorier av sökbegrepp ska, med avvikelse från sökbegreppen, inte hänvisas till sådana enskilda tekniska data, vilka som sådana kan användas som jämförelsebegrepp vid den automatiserade filtrering som ska inriktas på datatrafikflödet. Med kategori av sökbegrepp ska avses en exakt avgränsad muntlig beskrivning av de sökbegrepp som är relevanta med tanke på underrättelseuppdraget. Kategorierna av sökbegrepp ska innehålla flera uppgifter om underrättelseuppdraget utifrån vilka kommunikationen ska samlas in och lagras. Av kategorierna av sökbegrepp ska militärunderrättelsemyndigheten kunna välja de sökbegrepp som bäst hittar den väsentligaste kommunikationen med tanke på underrättelseuppdraget, vilka t.ex. inriktas på en organisation som utvecklar ett nytt vapensystem.

En kategori av sökbegrepp ska kunna användas i en situation där till samma helhet, som kan avgränsas exakt och definieras, hör flera sökbegrepp av samma typ av vilka man endast känner till en del när underrättelseinhämtning som avser datatrafik inleds. I stället för att inleda ett

nytt tillståndsförfarande alltid när ny information har erhållits genom underrättelseinhämtning som avser datatrafik, kunde man ansöka om tillstånd med en muntlig beskrivning av en sökbegreppsmängd, varvid nya enskilda sökbegrepp som skapas utifrån ny information skulle omfattas av det tidigare ansökta tillståndet. En kategori av sökbegrepp kunde vara t.ex. kommunikationsförbindelser i allmänhet mellan en viss grupp av personer som har specificerats i yrkandet. En faktor som förenar de personer som hör till gruppen kan vara t.ex. medlemskap i en viss militärt organiserad gruppering som specificerats i tillståndsyrkandet eller agerande i en viss arbetsuppgift i en sådan militär organisation som representerar en främmande stat.

När man med hjälp av underrättelseinhämtning som avser datatrafik en i gången får kännedom om teleadressrymder och andra utländska teleadresser som personer i gruppen använder, kan dessa användas som sökbegrepp. Medan underrättelseinhämtningen pågår ska man därmed från omfattande sökbegrepp som täcker ett stort antal teleadresser, med stöd av den information som inhämtas med underrättelseinhämtning som avser datatrafik, kunna övergå till mera exakta sökbegrepp samt dessutom till nya sökbegrepp som avslöjas utanför den ursprungliga adressmängden. Till följd av arten av föremålet för ett underrättelseuppdrag vore det nödvändigt att omedelbart få tillgång till nya sökbegrepp inom underrättelseinhämtningen. För att en viss persongrupps kommunikationsförbindelser ska kunna godkännas som kategori av sökbegrepp ska det förutsättas att grunderna för medlemskap i persongruppen har definierats tillräckligt exakt i yrkandet, att det har kunnat påvisas att gruppen är föremål för ett underrättelseuppdrag och att det yrkande som gäller gruppen också i övrigt uppfyller förutsättningarna för underrättelseinhämtning som avser datatrafik.

Som en tillåten kategori av sökbegrepp ska också kunna komma i fråga datakommunikationsförbindelser mellan ett visst i ansökan specificerat avgränsat geografiskt område och Finland. Det geografiska området i fråga ska kunna vara t.ex. en viss militär truppavdelnings kommandoplats, från vilken man utifrån annan underrättelseinformation vet att soldater, som är verksamma på en annan stats område, styrs. För att kommunikationsförbindelser som anknyter till ett visst geografiskt område ska kunna godkännas som kategori av sökbegrepp, ska man i yrkandet kunna påvisa betydelsen av det avgränsade geografiska området i fråga med tanke på ett underrättelseuppdrag. Yrkandet ska, om det behövs, också specificera de avgränsningar inom ramen för vilka konkreta sökbegrepp bildas för att underrättelseinhämtningen inte ska inriktas på sådan datatrafik som sänds från det geografiska området men som med tanke på underrättelseuppdraget är ovidkommande datatrafik.

Vidare ska som kategorier av sökbegrepp kunna komma i fråga t.ex. sådana sabotageprogramkoder som på förhand inte har specificerats i tillståndsansökan men som en viss främmande stats underrättelsetjänst använder i sitt cyberspionerі eller sådana nätadresser som på förhand inte har specificerats i tillståndsansökan och som underrättelsetjänsten i fråga använder som mellanhand i sitt cyberspionerі. Om koderna i ett sabotageprogram eller nätadresser specificeras i ett yrkande är det i dem fråga om sökbegrepp och inte kategorier av sådana. Behovet att yrka på att tillståndet ska vara mera generellt i fråga om de koder i sabotageprogram och nätadresser som används i cyberspionerі beror på att koderna och adresserna kan ändras medan underrättelseinhämtning som avser datatrafik pågår eller ny information kan erhållas om dem i den underrättelseinhämtning som avser datatrafik. En underrättelsetjänst som använder sabotageprogram i sitt cyberspionerі kan t.ex. ändra programmets kod så att den inte längre motsvarar den ursprungliga, varvid inte heller ett sådant enskilt sökbegrepp, för vilket domstolen har beviljat tillstånd till användning, längre identifierar koden. Om tillstånd kan yrkas och erhållas generellt i fråga om de sabotageprogramskoder som den i yrkandet nämnda underrättelsetjänsten använder (kategori av sökbegrepp), kunde underrättelseinhämtning som avser datatrafik inriktas på den ändrade koden utan avbrott.

På motsvarande sätt, om tillstånd till underrättelseinhämtning som avser datatrafik kunde yrkas endast för en enskild nätadress som används som mellanhand vid cyberspionerі (sökbegrepp), skulle av detta följa att den underrättelseinhämtning som avser datatrafik måste avbrytas, om den part som utövar spionerі styr trafiken längs en ny rutt. För att underrättelseinhämtning som avser datatrafik ska kunna utföras utan avbrott förutsätts att tillstånd ska ha yrkats och erhållits generellt för nätadresser (kategorier av sökbegrepp) som den i yrkandet nämnda underrättelsetjänsten använder som mellanhand i sitt cyberspionerі.

De uppgifter som kommer i fråga som tillåtna kategorier av sökbegrepp är det omöjligt att fastställa på förhand på ett uttömmande sätt. Således föreslås det att domstolspraxis ska få klargöra vilken mängd av till varandra anknutna uppgifter som är tillräckligt exakt för att kunna komma i fråga som kategori av sökbegrepp. När domstolen godkänner att en viss kategori av sökbegrepp får användas, kan den ställa sådana begränsningar och mera exakta villkor för användningen som föreslås nedan i 9 punkten i detta moment.

Eftersom det i domstolens tillståndsgodkännande som gäller kategori av sökbegrepp är fråga om att Försvarsmaktens underrättelsetjänst, i egenskap av den som genomför underrättelseinhämtning som avser datatrafik, ges begränsad rätt att själv forma de konkreta sökbegrepp som ska användas i underrättelseinhämtning som avser datatrafik, föreligger det ett behov att inrikta en särskilt noggrann övervakning på denna del av verksamheten. Föremål för övervakningen ska vara att fastställandet av konkreta sökbegrepp görs inom ramen för den kategori av sökbegrepp som domstolen har godkänt i sitt beslut. Om övervakningen av underrättelseverksamheten ska föreskrivas i en särskild lag. I praktiken ska justeringen av sökbegreppen inom kategorierna av sökbegrepp vid Försvarsmaktens underrättelsetjänst i första hand övervakas av den i tillståndet nämnda tjänsteman som leder och övervakar underrättelseinhämtningen i datatrafik hos andra än statliga aktörer och som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning.

I tillståndsyrkandet och beslutet ska också nämnas motiveringar för de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas inom underrättelseinhämtning som avser datatrafik. De sökbegrepp som ska användas vid underrättelseinhämtning som avser datatrafik ska i regel vara tekniska data, vilkas anknytning till den verksamhet som är föremål för underrättelseinhämtning som avser datatrafik inte nödvändigtvis verkar uppenbar. Den som framställer yrkandet ska därmed motivera för domstolen vilken förbindelsen mellan sökbegreppen och ett underrättelseuppdrag är, varför det antas att genom användning av sökbegrepp erhålls information om verksamheten i fråga och hurdan information som sannolikt erhålls genom användning av sökbegreppen. Om ett sökbegrepp t.ex. är en IP-adressrymd, bör det redogöras för på vilka grunder datatrafik som anknyter till ett underrättelseuppdrag antas finnas i IP-adressrymden i fråga och hurdan denna trafik i så fall är. Om yrkandet gäller en kategori av sökbegrepp, ska på motsvarande sätt motiveras vilken förbindelsen är mellan den valda kategorin av sökbegrepp och den verksamhet som ett underrättelseuppdrag gäller som ska redas ut med underrättelseinhämtning som avser datatrafik, hur man har för avsikt att bilda de tekniska sökbegreppen inom ramen för kategorin av sökbegrepp och hurdan information man har för avsikt att inhämta med hjälp av de sökbegrepp som bildas.

Sökbegreppen ska alltid vara så exakta som möjligt så att den utomstående datatrafik som råkar bli behandlad av militärunderrättelsemyndigheten är så liten som möjligt eller att det inte alls förekommer sådan. Skyldigheten att fastställa sökbegrepp och kategorier av sökbegrepp så att de så exakt som möjligt når sitt mål kan härledas redan av principen om minsta olägenhet och proportionalitetsprincipen. Enligt principen om minsta olägenhet får man inte ingripa i

någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenhet än vad som är nödvändigt för att utföra uppdraget.

Enligt 5 punkten ska i yrkandet och beslutet meddelas de delar av kommunikationsnätet som överskrider Finlands gräns, såsom trådfibrer, som underrättelseinhämtning som avser datatrafik ska inriktas på. Till exempel genom att inrikta underrättelseinhämtning som avser datatrafik på enskilda fibrer ställs en betydande del av den datatrafik som överskrider Finlands gränser utanför informationsinhämtningen, vilket för sin del också effektiverar och inriktar den underrättelseinhämtning som avser datatrafik på korrekt sätt.

Insamlandet av datatrafik med hjälp av sökbegrepp ska inte kunna gälla hela kommunikationsnätet, utan insamlandet av datatrafik ska i varje situation få gälla en så snäv del som möjligt av nätet. Den som anför ett yrkande ska vara skyldig att i sitt tillståndsyrkande så exakt som möjligt definiera de datatrafiktrådar eller, om möjligt, de fibrer eller våglängder, där sökbegreppen ska användas vid underrättelseinhämtning som avser datatrafik på den datatrafik som flödar i trådarna. Den uppgift om kommunikationsnätsdel som förutsätts i yrkandet och beslutet ska beroende på fallet redas ut antingen genom behandling av tekniska data i datatrafiken enligt den föreslagna 63 § eller med hjälp av dataöverförarens biståndsskyldighet enligt den föreslagna 95 §. Mest allmänt vid utredningen av kommunikationsnätsdel kommer en kombination av de nämnda utredningsmetoderna att användas.

Vid identifiering av en kommunikationsnätsdel ska den behandling av tekniska data om vilken ska föreskrivas i 63 § och dataöverförarens skyldighet att lämna ut uppgifter vara anknutna. Vid dirigeringen av annan datatrafik än den som avses i 63 § ska de uppgifter som erhållits av dataöverföraren kunna verifieras med hjälp av behandling av datatrafikens tekniska data. Vidare ska genom denna verksamhet kunna fås sådan ny information som dataöverföraren inte innehar och som kan användas för att utesluta viss datatrafik. Användningen av uteslutande information gör det möjligt att informationsinhämtning som baserar sig på sökbegrepp i underrättelseinhämtning som avser datatrafik som genomförs i en senare fas inte riktas mot en mera omfattande del av datanätet än vad som är nödvändigt.

I yrkandet och beslutet ska nämnas motiveringar för den kommunikationsnätsdel som underrättelseinhämtning som avser datatrafik ska inriktas på. Försvarsmaktens underrättelsetjänst ska i sitt yrkande redogöra för varför och på vilka grunder det kan antas att datatrafik som anknyter till verksamhet som är föremål för ett underrättelseuppdrag rör sig i den datanätsdel som yrkandet gäller.

Enligt momentets 6 punkt ska i yrkandet och beslutet nämnas hur länge beslutet om underrättelseinhämtning som avser datatrafik är i kraft med angivande av klockslag. Liksom i fråga om övriga metoder för underrättelseinhämtning, ska de inhämtade uppgifterna hela tiden bedömas och underrättelseinhämtningen ska avbrytas när målet för den underrättelseinhämtning som avser datatrafik har uppnåtts.

Enligt 7 punkten ska för underrättelseinhämtning som avser datatrafik enligt tillståndet nämnas den tjänsteman vid Försvarsmaktens underrättelsetjänst som leder och övervakar användningen av metoder för underrättelseinhämtning och som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning. Den tjänsteman som leder och övervakar och är särskilt förtrogen med användningen av metoder för underrättelseinhämtning ska i första hand övervaka också användningen av de sökbegrepp som avses i 3 punkten och den justering av sökbegrepp som görs inom kategorierna av sökbegrepp.

Enligt 8 punkten ska i yrkandet och beslutet också anges begränsningar och villkor för underrättelseinhämtning som avser datatrafik. Domstolen ska i sitt beslut kunna ställa begränsningar och villkor för den underrättelseinhämtning som avser datatrafik. Om man känner till sådana begränsningar och villkor redan när yrkandet uppgörs, är det skäl att skriva in dem i yrkandet. Begränsningar och villkor ska kunna ställas t.ex. för hur Försvarsmaktens underrättelsetjänst får bilda sökbegrepp inom ramen för de kategorier av sökbegrepp för vilka domstolen beviljar tillstånd.

**69 §.** *Genomförande av den koppling som behandlingen av tekniska data och underrättelseinhämtning som avser datatrafik förutsätter.* Enligt paragrafen ska en anslutning enligt det tillstånd som avses i 64, 66 och 68 § till en enskild fiber i en tråd som överskrider Finlands gränser göras av den som utför en koppling med bistånd av den dataöverförare som anvisas i domstolens tillstånd. Verkställande ska avse att den som utför kopplingen styr vidare till Försvarsmaktens underrättelsetjänst den datatrafik som flödar i en fysisk anslutning, som stämmer överens med tillståndet, från den kommunikationsnätsdel som dataöverföraren innehar. Den som utför kopplingen ska också försäkra sig om att Försvarsmaktens underrättelsetjänst under hela tillståndets giltighetstid har tillträde endast till den del av ett kommunikationsnät som stämmer överens med det tillstånd som avses i 64, 66 och 68 § och att Försvarsmaktens underrättelsetjänst inte kommer åt att använda datatrafik som flödar i andra förbindelser, såsom fibrer eller våglängder, för sin underrättelseinhämtning.

När den som utför kopplingen utför sina uppgifter enligt paragrafen, ska särskild uppmärksamhet ägnas att datasäkerheten och kunnandet i datasäkerhet är höga.

Enligt 2 mom. ska den som utför kopplingen överlåta vidare till Försvarsmaktens underrättelsetjänst datatrafiken i den kommunikationsnätsdel som stämmer överens med tillståndet. På detta sätt får militärunderrättelsemyndigheten inte direkt tillträde till den kommunikation som rör sig i andra delar av kommunikationsnätet.

**70 §.** *Tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning.* Militärunderrättelsemyndigheterna i Finland har det kunnande och de resurser som behövs för det tekniska genomförandet av underrättelseinhämtning som avser datatrafik. Skyddspolisen har behov av den information som inhämtas med underrättelseinhämtning som avser datatrafik. Med tanke på en effektiv användning av resurserna är det emellertid inte ändamålsenligt att flera olika myndigheter har teknisk beredskap att genomföra underrättelseinhämtning som avser datatrafik. Enligt 1 mom. ska militärunderrättelsemyndigheterna samla in kommunikation ur datatrafiken också för en aktör som står utanför försvarsförvaltningen.

Med tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning, som avses i 1 mom. 1 punkten, ska avses inhämtande av tekniska data för att den underrättelseinhämtning som avser datatrafik ska kunna inriktas. Militärunderrättelsemyndigheterna ska kunna inhämta tekniska data ur datatrafiken för adekvat genomförande av underrättelseinhämtning som avser datatrafik för att göra en teknisk analys, såsom det föreskrivs i 63 §. Sådana tekniska data ska också kunna inhämtas på begäran av skyddspolisen för genomförande av den underrättelseinhämtning som avser datatrafik som skyddspolisen behöver. I denna situation ska Försvarsmaktens underrättelsetjänst också inhämta tillstånd av domstolen, fastän analysen ska göras på uppdrag av skyddspolisen. Vid behandlingen av tekniska data är det inte fråga om att inhämta något betydande tillstånd som kräver övervägning av domstolen. Det är fråga om att inhämta tekniska data för att underrättelseinhämtning som avser datatrafik ska kunna inriktas korrekt, och med behandlingen av tekniska data ska det inte inhämtas information om meddelandenas innehåll. Domstolens prövning ska begränsas till hur tekniska

data ska behandlas, från vilken kommunikationsnätsdel de ska inhämtas och tillståndets giltighetstid.

Enligt 2 punkten ska med tekniskt genomförande av underrättelseinhämtning som avser datatrafik avses tekniskt inhämtande av data för skyddspolisens räkning i enlighet med ett tillstånd som domstolen har beviljat. Försvarsmaktens underrättelsetjänst ska vara teknisk genomförare av underrättelseinhämtning för skyddspolisens räkning. I dessa fall ska Försvarsmaktens underrättelsetjänst inhämta datatrafik enligt ett tillstånd som skyddspolisen har fått av domstolen i den del av kommunikationsnätet som avses i tillståndet, inhämta datatrafik som stämmer överens med sökbegrepp och kategorier av sökbegrepp i datatrafiken och överlåta den vidare till skyddspolisen för fortsatt behandling.

I den underrättelseinhämtning som avser datatrafik ska varje myndighet vara ansvarig för att hos behörig domstol ansöks om det tillstånd som behövs vid underrättelseinhämtning som avser datatrafik som riktas mot annat än datatrafikens tekniska data. Vid tekniskt genomförande för skyddspolisens räkning ska Försvarsmaktens underrättelsetjänst endast inhämta data ur datatrafiken enligt tillståndsvillkoren för en annan myndighets räkning. Inhämtade data ska överlåtas till skyddspolisen, som ska behandla den inhämtade uppgifterna i enlighet med sina egna uppdrag.

I paragrafens 2 mom. föreslås en hänvisningsbestämmelse till lagen om civil underrättelseinhämtning avseende datatrafik. Bestämmelser om den underrättelseinhämtning som avser datatrafik som ska genomföras för skyddspolisens räkning ska ingå i 10 § i lagen.

Enligt 3 mom. ska Försvarsmaktens underrättelsetjänst inte ha tillgång till innehållet i de meddelanden som ingår i den datatrafik som inhämtats genom underrättelseinhämtning som avser datatrafik för skyddspolisens räkning och underrättelsetjänsten ska inte heller kunna behandla dem i efterhand. Detta gäller emellertid inte den tekniska analys som gjorts utgående från datatrafikens tekniska data på uppdrag av skyddspolisen. Adekvat inriktning av den underrättelseinhämtning som avser datatrafik kräver aktuell information om längs vilka rutter datatrafikens rör sig i kommunikationsnätet. I ruttdirigeringen kan det ske snabba förändringar, vilket gör att det med tanke på underrättelsemyndigheternas verksamhet vore ändamålsenligt att underrättelsemyndigheterna till sitt förfogande har en så omfattande och aktuell bild som möjligt av hur datatrafiken rör sig.

**71 §.** *Utlämnande av uppgifter om ett skadligt datorprogram till företag och sammanslutningar.* Enligt paragrafen ska uppgifter om ett skadligt datorprogam eller kommando kunna överlåtas till företag och sammanslutningar, om överlåtelse av uppgifterna behövs för att trygga försvaret av landet, skydda den nationella säkerheten eller trygga företagets eller sammanslutningens intressen. Dessutom ska Försvarsmaktens underrättelsetjänst kunna överlåta uppgifter om ett skadligt datorprogram till en behörig myndighet, såsom Kommunikationsverket.

I Finland deltar ett stort antal företag och andra sammanslutningar i försvaret av staten och samhället och utvecklandet av detta och dessa producerar också tjänster med anknytning till statens säkerhet och samhällets vitala funktioner. För att kontinuiteten i dessa tjänster ska kunna garanteras är det viktigt att de uppgifter som genom underrättelseinhämtning som avser datatrafik har erhållits om utvecklade skadliga datorprogram eller kommandon kan ges också till företagen och sammanslutningarna.

Ett syfte med underrättelseinhämtning som avser datatrafik är att förbättra samhällets skydd mot tekniskt avancerade datanätsattacker, t.ex. cyberspionieri. Det kan bedömas att underrät-

telseinhämtning som avser datatrafik kommer att resultera i en stor mängd observationer och information om skadliga datorprogram och datorkommandon som används vid datanätsattacker. När avancerade datanätsattacker utöver mot myndigheterna också kan rikta sig mot företag och sammanslutningar, är det med tanke på det övergripande skyddandet av det finska samhället viktigt att uppgifter om de sabotageprogram som används vid attackerna i så vidsträckt omfattning som möjligt kan överlåtas till potentiella mål för attackerna. Genom att föreskriva om rätt att överlåta dylika uppgifter kan man garantera möjligheter för företagen och sammanslutningarna att vidta sådana åtgärder för att sörja för sin datasäkerhet om vilka föreskrivs i 272 § i lagen om tjänster inom elektronisk kommunikation. Åtgärder i överenstämmelse med bestämmelsen i fråga kan innehålla bl.a. automatisk utredning av innehållet i ett meddelande, automatiskt förhindrande eller begränsande av förmedling och mottagande av meddelanden samt automatiskt avlägsnande ur meddelanden av skadliga datorprogram som äventyrar datasäkerheten.

Det är i allmänhet mest effektivt att identifiera tekniska nätattacker så nära ett system, som potentiellt kan vara mål för en attack, som möjligt och på åtgärd av systemets egna underhållsansvariga. Det finns emellertid situationer där de eventuella målen är många eller underhållet av de potentiella målsystemen har lagts ut på entreprenad till någon sådan utländsk part att det inte är möjligt att överlåta detaljerad information om avvärjningsindikatorer utan att den nationella säkerheten äventyras. Då ska information om attacker eller förberedande åtgärder kunna inhämtas genom underrättelseinhämtning som avser datatrafik.

Efter ett inträffat datasäkerhetsintrång kan man försöka identifiera en avvikelse utifrån ett trafikflöde av en mängd egenskaper som orsakats av ett sabotageprogram eller ett skadligt kommando. Däremot är det ofta inte möjligt att göra avvärjandet på förhand med stöd av enbart rubrikuppgifter eller särdrag i trafikflödet i datatrafiken, eftersom den datatrafik som förutser intrånget strävar efter att maskera sig till sedvanlig kommunikation. Därför ska det föreskrivas om ett undantag som gör det möjligt att söka i innehållet i trafik som innehåller ett skadligt datorprogram eller kommando.

Med skadlighet avses här äventyrande av den tekniska datasäkerheten, dvs. ett datorprogram eller kommando som strävar efter att stjäla information, ändra information utan att ha rätt till det eller skada målsystemets verksamhet. Som målsystem ska anses vilket som helst digitalt system, också själva nätet, dvs. de nätanordningar som styr datatrafiken samt de anordningar som styr processerna i den reella världen. Eftersom ett sökbegrepp inte ska vara ett ord i ett naturligt språk, utan någon teknisk teckensträng, ska kravet på avgränsning av vilken datatrafik som blir utsatt för automatisk jämförelse inte vara lika strängt som vid innehållsinhämtning som riktas mot det semantiska innehållet i en statlig aktörs kommunikation.

Enligt bestämmelsen ska uppgifter om skadliga datorprogram och datorkommandon få överlåtas trots sekretessbestämmelserna. Dylika uppgifter ska uppenbarligen kunna vara sekretessbelagda främst utgående från 24 § 1 mom. 7 eller 9 punkten i lagen om offentlighet i myndigheternas verksamhet (621/1999). Enligt den först nämnda bestämmelsen är sekretessbelagda handlingar bl.a. sådana som gäller data- och kommunikationssystemens skyddsarrangemang och som påverkar genomförandet av dem, om det inte är uppenbart att utlämnandet av uppgifter ur en sådan handling inte äventyrar genomförandet av syftet med skyddssystemen. Om information om ett skadligt datorprogram eller datorkommando blir offentlig kan det åtminstone i en del fall äventyra realiserandet av syftet med skyddsarrangemangen, eftersom den part som använder sabotageprogrammet eller sabotagekommandot i och med att informationen blir offentlig kan dra slutsatser om myndigheternas förmåga att upptäcka och avvärja attacker. Detta kan i sin tur leda till att sabotageprogrammet eller sabotagekommandot ändras eller vidareut-

vecklas så att det blir svårare att upptäcka än tidigare. Eftersom det är möjligt att använda ett modifierat sabotageprogram också för sådan verksamhet som direkt äventyrar statens säkerhet, kan som grund för sekretess komma i fråga också 24 § 1 mom. 9 punkten i lagen om offentlighet i myndigheternas verksamhet. Enligt bestämmelsen i fråga är de av skyddspolisens och andra myndigheters handlingar sekretessbelagda som gäller upprätthållande av statens säkerhet, om det inte är uppenbart att utlämnande av uppgifter ur dessa inte äventyrar statens säkerhet. Även om offentliggörandet av information om ett sabotageprogram äventyrar ovan nämnda intressen, äventyras de inte nödvändigtvis om information överlåts till en enskild organisation som är föremål för en datanätsattack. Om detta är fallet, ska information kunna överlåtas till målorganisationen för skyddande av den nationella säkerheten eller för tryggande av målorganisationens intressen.

Bestämmelsen ska till sin art vara tillåtande, inte förpliktande. Beslutsfattandet om överlåtelse av en uppgift ska grunda sig på prövning och intresseövervägning från fall till fall. I en del situationer kan skäl som anknyter till försvaret av landet eller den nationella säkerheten hindra att information överlåts, även om erhållandet av informationen i sig vore behövlig för ett företag eller en sammanslutning för att de ska kunna säkerställa sina intressen. Syftet med bestämmelsen ska inte vara att överföra ansvaret för företagens och sammanslutningarnas datasäkerhet till underrättelsemyndigheterna, utan göra det möjligt att underrättelsemyndigheterna för sin del kan stöda företagens och sammanslutningarnas åtgärder för att skydda sig mot datanätsattacker.

För överlåtelse av information om ett skadligt datorprogram eller datorkommando ska det finnas tre alternativa grunder: att trygga försvaret av landet, att skydda den nationella säkerheten och att skydda ett företags eller en sammanslutnings intresse. Grunderna för överlåtelse av information kan förenas i fall där det är fråga om t.ex. att upprätthålla samhällets vitala infrastruktur eller ett företag eller en sammanslutning som har betydelse med tanke på hela samhällsekonomin. Av det att grunderna är alternativa följer emellertid att information inom övervägda gränser kan överlåtas utan hänsyn till om företaget eller sammanslutningen har sådan betydelse eller inte.

Överlåtelse av information till en behörig myndighet kommer i fråga när information om ett skadligt datorprogram eller datorkommando har mera vidsträckt betydelse med tanke på samhället. I dylika situationer sprids informationen bäst genom förmedling av någon annan än underrättelsemyndigheterna, t.ex. Kommunikationsverket. På detta sätt kan man också garantera att underrättelseverksamheten inte äventyras.

## 5 kap. Skyddande av militär underrättelseinhämtning samt tryggande av tjänstemän och informationskällor

**72 §.** *Skyddande av militär underrättelseinhämtning.* I paragrafen ska det föreskrivas om hur det kan förhindras att den militära underrättelseinhämtningen avslöjas. Utförandet av ett underrättelseuppdrag, informationsinhämtning och de metoder som ska användas måste vid behov kunna skyddas för att det ska förhindras att de avslöjas.

Enligt 1 mom. ska vid informationsinhämtningen kunna användas falska, vilseledande eller förtäckta uppgifter för att skydda ett underrättelseuppdrag och utövandet av befogenheter, när detta behövs för att förhindra att militär underrättelseinhämtning avslöjas. Motsvarande behövlighetsförutsättning finns i förslaget till paragraf om skyddande av civil underrättelseinhämtning. Tröskeln ska anses tillräcklig med beaktande av syftet med och föremålen för militär underrättelseinhämtning. Verksamhetens art skiljer sig betydligt från användningen av

hemliga metoder för inhämtande av information enligt 5 kapitlet i polislagen, där det föreskrivs om en nödvändighetsförutsättning vid skyddandet av informationsinhämtningen.

Underrättelseinhämtningen kan också skyddas i datanäten, t.ex. i samband med anskaffning av olika tjänster. Registrering i en viss elektronisk tjänst och anskaffning av tjänster kan förutsätta s.k. stark elektronisk autentisering. En stark elektronisk identifikator kan förutsätta att falska, vilseledande eller förtäckta uppgifter används för att en identifikator ska erhållas.

Behörigheten att göra anteckningar ska innehas av militärunderrättelsemyndigheterna, även om anteckningarna i praktiken ska göras i samarbete med parternas registeransvariga inom de gränser som registrets systematik och tekniska lösningar ställer. Genom denna lösning försätts inte en enskild tjänsteman i fara men det säkerställs att t.ex. att en så liten grupp som möjligt känner till skyddade informationskällors personuppgifter. Bestämmelsen möjliggör inte att anteckningar görs genom Försvarsmaktens underrättelsetjänsts direktförbindelse. För den militära underrättelseverksamhetens del är det centralaste registret i praktiken befolkningsdatasystemet, även om man också kan bli tvungen att göra anteckningar i andra myndigheters eller privata aktörers register. Varje enskild åtgärd ska det överenskommas om särskilt. De praktiska samarbetsformerna kommer av säkerhetsskäl att utvecklas inom tillämpningspraxis.

Enligt 2 mom. ska en registeranteckning som avses i 1 mom. rättas när förutsättningarna enligt det momentet inte längre finns.

**73 §.** *Beslut om skyddande av militär underrättelseinhämtning.* Enligt 1 mom. ska beslutet om de registeranteckningar som ska användas vid skyddandet av underrättelseinhämtningen fattas av Huvudstabens underrättelsechef.

Enligt 2 mom. beslutar en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman om annat skyddande av underrättelseinhämtning.

Enligt 3 mom. ska Huvudstabens underrättelsechef ansvara för att registeranteckningarna görs, för att en förteckning förs över registeranteckningar och handlingar, övervaka användningen av dem samt se till att registeranteckningarna rättas. Det ändamålsenligaste vore att den myndighet som beslutar om att upprätta handlingar och göra registeranteckningar också ansvarar för att de förtecknings-, övervaknings- och rättelseskyldigheter som gäller dem uppfylls. En rättelse av registeranteckningarna ska göras när anteckningarna inte längre behövs för att skydda underrättelseinhämtningen.

De åtgärder som avses i 72 § 1 mom. ska inte få inriktas på en förteckning som avses i detta moment.

**74 §.** *Tryggande av en tjänsteman som använder en metod för underrättelseinhämtning.* Enligt 1 mom. ska en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman få besluta att en tjänsteman som använder en metod för underrättelseinhämtning förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att tjänstemannens säkerhet ska kunna tryggas. Bestämmelsen gäller så kallad säkerhetsavlyssning och säkerhetsobservation. Enligt straffbestämmelsen om avlyssning är det inte straffbart att i hemlighet spela in sina egna samtal. Användningen av sådana anordningar som avses i momentet utgör inte heller annars sådan orättmätig verksamhet som kan leda till straffansvar för olovlig avlyssning eller observation. Säkerhetsavlyssning och säkerhetsobservation får riktas endast mot personer som är i interaktion med en tjänsteman som genomför en täckoperation eller bevisprovokation genom köp. Ut-

trycket "avlyssning och observation" avser att man beroende på fallet kan använda antingen en anordning som möjliggör avlyssning eller observation eller en anordning som möjliggör både avlyssning och observation.

Enligt 1 mom. ska en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman dessutom få besluta att en tjänsteman vid militärunderrättelsemyndigheterna som reder ut huruvida en person som ska rekryteras till informationskälla till sina personliga egenskaper är lämplig som informationskälla, får förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att tjänstemannens säkerhet ska kunna tryggas.

Bestämmelsen gör det möjligt att trygga säkerheten för en tjänsteman vid militärunderrättelsemyndigheten vid användningen av informationskällor samt att informationskällan och tjänstemannen kan bygga upp en förtrolig relation i de förberedande åtgärderna. En tjänsteman vid militärunderrättelsemyndigheten kan vid användning av informationskällor utsätta sig själv för fara för liv och hälsa av samma nivå som t.ex. i en täckoperation. Detta gäller i synnerhet situationer där det inte ännu föreligger någon säkerhet om hur den som ska rekryteras till informationskälla förhåller sig till en tjänsteman som närmar sig denna person.

Enligt 2 mom. får avlyssningen och observationen upptas. Upptagningarna ska utplånas så snart de inte behövs för att trygga tjänstemannens 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 ska innehåll begränsningar för bevarande och användning av upptagningar av säkerhetsavlyssning och säkerhetsobservation. Dessa får inte bevaras och användas för andra ändamål än de som nämns i bestämmelsen. Det kan i dessa fall vara fråga om t.ex. att en tjänsteman vid militärunderrättelsemyndigheten har utsatts för våld, att han eller hon har varit tvungen att bruka våld eller att någon har orsakats skada i samband med användningen av en metod för underrättelseinhämtning. I dessa fall kan upptagningarna behövas vid behandlingen av ett brottmål eller skadeståndsärende.

**75 §.** *Tryggande av informationskällor.* I paragrafen ska det föreskrivas om tryggandet av informationskällor. Militärunderrättelsemyndigheterna har i princip skyldighet att sörja för informationskällornas säkerhet om så behövs både medan informationsinhämtning pågår och efter det. Befogenheten att trygga informationskällor ska dock inte ersätta det vittnesskyddsprogram som avses i lagen om vittnesskyddsprogram (88/2015). Om en informationskälla behöver skyddas under en längre tid och ett allvarligt hot mot liv eller hälsa riktas mot personen och hotet inte effektivt kan avvärjas med andra åtgärder, är det motiverat att överväga att inleda ett vittnesskyddsprogram för informationskällan.

Enligt 1 mom. ska militärunderrättelsemyndigheterna med en informationskällas samtycke kunna övervaka dennes bostad, eller något annat utrymme eller en plats av ett annat slag 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 erhållandet av samtycke försäkrar man sig om att informationskällan också själv vill bli tryggad. Utomstående behöver inte upplysas om att informationskällan tryggas.

I momentet ska det möjliggöras att olika säkerhetssystem som behövs för att trygga en informationskälla, såsom t.ex. övervakningskameror och rörelsedetektorer, kan installeras i den skyddsbehövande informationskällans bostad och i dess omedelbara närmiljö. Med annat utrymme som informationskällan använder för boende ska avses t.ex. hotellrum samt andra platser där informationskällan är bosatt vid tidpunkten i fråga.

I motsats till vad som är fallet vid optisk observation, ska övervakningen inte ske utan objektets vetskap och inte i syfte att inhämta information. Syftet med övervakningen ska i stället vara att trygga informationskällan, men indirekt ska med tryggandet av informationskällan också sammanhänga ett syfte att inhämta information t.ex. om vem som rör sig i området.

Övervakningen ska inte få utföras, om den inte behövs för att avvärja en fara som hotar informationskällans liv och hälsa. Med detta ska avses att åtminstone en potentiell fara ska riktas mot informationskällans liv och hälsa.

Bestämmelsen ska också gälla sådana situationer där anordningar som installerats i hemmet hos den som ska skyddas eller i dess omedelbara närmiljö också sträcker sig över någon annans hemfridsskyddade område, också om det inte gäller kärnområdet. En dylik situation kan gälla ett höghus, där en säkerhetskamera också tar foton på trappuppgången som är gemensam för dem som bor i husbolaget eller ett radhus, där fotograferandet också kan omfatta gemensamma gårdsområden.

Tryggandet av informationskällans säkerhet förutsätter att utomstående inte informeras om kameraövervakning och annan övervakning för undvikande av risken för avslöjande och för skyddande av informationskällans liv och hälsa.

Enligt 2 mom. ska övervakningen avslutas utan dröjsmål, om den inte längre behövs för att avvärja en fara som hotar informationskällans liv eller hälsa. Detta betyder att när det inte finns någon grund för att trygga informationskällan, ska säkerhetsåtgärderna avslutas omedelbart.

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 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.

Upptagningarna får inte bevaras och användas för andra ändamål än de som nämns i bestämmelsen. I dessa fall kan det vara fråga om att en informationskälla har utsatts för våld och myndigheten omedelbart har ingripit i verksamheten. Ifall åtal väcks mot myndigheten i en sådan situation, kan de upptagningar som uppkommit vid tryggandet av informationskällans säkerhet användas som en utredning som påvisar att någon är oskyldig eller skyldig. I dessa fall kan upptagningarna behövas vid behandlingen av ett brottmål eller skadeståndsärende. Eftersom det är fråga om en säkerhetsbefogenhet och inte om användning av en metod för underrättelseinhämtning, är det inte fråga om att använda information som erhållits med en metod för underrättelseinhämtning i en straffprocess, utan upptagningarna har uppkommit i ett annat syfte. Straff- och skadeståndsbehandlingen kan dock förutsätta förhandling inom stängda dörrar.

I paragrafens 4 mom. ska det föreskrivas om tryggandet av en informationskällas säkerhet genom säkerhetsavlyssning och säkerhetsobservation. I den militära underrättelseinhämtningen

behöver informationskällor värvas i kärnan av den verksamhet som hotar landets försvar och den nationella säkerheten, vilket gör att när en person ger sitt samtycke till att bli en informationskälla utsätter personen sitt eget liv och sin hälsa för fara. Informationskällorna har inte heller utbildning i användningen av maktmedel, vilket gör att det är ytterst viktigt att det med myndighetsåtgärder sörjs för deras säkerhet.

Det ska vara tillåtet att förse en informationskälla med sådana tekniska anordningar som möjliggör säkerhetsavlyssning eller säkerhetsobservation endast kortvarigt i sådana situationer där informationskällans säkerhet inte kan garanteras tillräckligt effektivt med andra myndighetsåtgärder eller där det är i det närmaste omöjligt att trygga informationskällans säkerhet med andra metoder. Med formuleringen ”i ett enskilt fall” ska uttryckligen avses att åtgärden ska begränsas till en enskild händelse. Åtgärdens nödvändighet uttrycker att en informationskällas säkerhet inte kan tryggas med någon annan metod och att det inte med någon annan metod går att få information om militär verksamhet eller verksamhet som hotar den nationella säkerheten.

Den som fattar beslutet ska vara tillräckligt förtrogen med användningen av informationskällor. Detta uttrycks bl.a. av det att beslut om åtgärden ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Utöver beslut av en militärjurist eller en annan tjänsteman ska säkerhetsavlyssningen och säkerhetsobservationen basera sig på samtycke av informationskällan. Informationskällan ska till sina personliga egenskaper vara sådan att han eller hon kan agera naturligt också med en teknisk anordning som möjliggör säkerhetsavlyssning på sig.

Syftet med denna åtgärd ska endast vara att trygga informationskällans säkerhet. Således får bestämmelserna om teknisk avlyssning och optisk observation inte kringgås med detta. Detta uttrycks genom det att avlyssnings- och observationsupptagningarna ska utplånas så snart de inte behövs för att trygga informationskällans säkerhet.

I 5 mom. ska det föreskrivas om tryggandet av informationskällan för förhindrande av att informationsinhämtningen avslöjas och för skyddande av informationskällans liv och hälsa. Vid det tryggande av informationskällan som avses i momentet ska det vara fråga om att falska, vilseledande och förtäckta uppgifter eller registeranteckningar eller falska handlingar ges informationskällan för att användas en kort tid.

I en sådan situation som avses i momentet ska det vara fråga om att trygga lämnandet av uppgifter som informationskällan har inhämtat, inte om utövande av en befogenhet. Vid användningen av en informationskälla ska informationskällan agera som sig själv och utifrån sin ställning ska han eller hon ha rätt att få tillgång till dessa uppgifter. I dessa situationer ska det uttryckligen vara frågan om att lämna uppgifter till militärunderrättelsemyndigheterna och att trygga informationskällans liv och säkerhet i denna situation.

I de situationer som avses i momentet ska en förutsättning vara att det är nödvändigt att en informationskälla ges falska, vilseledande och förtäckta uppgifter eller registeranteckningar eller att falska handlingar får upprättas för att användas av informationskällan för att uppgifter ska fås med tanke på ett underrättelseuppdrag samt att det är nödvändigt att använda falska, vilseledande och förtäckta uppgifter eller registeranteckningar eller falska handlingar för att informationskällans liv och hälsa ska kunna skyddas.

Tryggandet av en informationskällas säkerhet ska kunna komma i fråga t.ex. i en situation där informationskällan innehar uppgifter som är ytterst viktiga med tanke på ett militärunderrättel-

seuppdrag och uppgifterna inte kan föras över till militärunderrättelsemyndigheten på annat sätt än genom ett möte med informationskällan. Dessutom ska överskridande av statsgränsen genom användning av t.ex. falska handlingar vara nödvändigt för att informationskällans liv och hälsa ska kunna skyddas.

Omnämnandet av ”i ett enskilt fall” i momentet ska utöver till nödvändighetsförutsättningen också hänvisa till att det är fråga om en med tanke på den militära underrättelseinhämtningen ytterst betydande situation. Vidare ska ett enskilt fall hänvisa till att det inte är fråga om långvarig användning av de uppgifter och handlingar som nämns i momentet.

Registeranteckningarna kan vara sådana som t.ex. stöder en annan identitet. För att risken för avslöjande ska kunna undvikas är det viktigt att den berättelse som stöder den andra identiteten för den person som ska skyddas är så trovärdig och enhetlig som möjligt. En tillfällig täckidentitet ska inte kunna spåras till den egentliga identiteten hos den person som ska skyddas, eftersom utgångspunkten ska vara att endast en viss tjänsteman vid Försvarsmaktens underrättelsetjänst och Huvudstabens underrättelsechef ska känna till den riktiga identiteten för den som ska skyddas. Det ska därmed inte vara fråga om att byta identitet, eftersom identiteten för den som ska skyddas förblir i kraft fastän den som ska skyddas övergår till att använda en täckidentitet. När behovet av skydd har upphört ska den som behövde skydd igen kunna ta i användning sin riktiga identitet. Bestämmelsen ska möjliggöra att registeranteckningar och handlingar som stöder täckidentiteten förs in i t.ex. befolkningsdatasystemet. Med stöd av bestämmelsen ska de registeranteckningar som behövs också kunna göras i uppgifterna om den riktiga identiteten för den som ska skyddas. I ett långvarigare behov av skydd ska man som sista metod kunna överväga att inleda ett vittnesskyddsprogram, om vilket bestäms i lagen om vittnesskyddsprogram (65/2014).

Vid tryggandet av en informationskällas säkerhet ska uppmärksamhet fästas vid den handledning som anknyter till informationskällans säkerhet, såsom att undvika vissa platser samt beteendet i de sociala medierna så att personens verkliga identitet inte avslöjas för utomstående. I praktiken ska det ingå i den allmänna försiktigheten att den som skyddas inte deltar i kriminell verksamhet. Skyddandet av en informationskälla inverkar inte på hur det straffrättsliga ansvaret förverkligas, vilket gör att delaktighet i kriminell verksamhet i praktiken kan omöjliggöra skyddandet, eftersom den som ska skyddas i detta fall blir tvungen att uppträda med sin verkliga identitet.

Enligt den sista meningen i momentet ska en registeranteckning rättas när förutsättningarna enligt detta moment inte längre finns. Detta innebär att när det inte längre är nödvändigt att trygga informationskällans säkerhet för att få uppgifter samt för att skydda informationskällans liv och hälsa, ska falska, vilseledande och förtäckta uppgifter eller registeranteckningar rättas och informationskällan fråntas falska handlingar. Det är inte ändamålsenligt att en informationskälla kan använda de uppgifter och handlingar som avses i momentet för annat än för att lämna uppgifter till militärunderrättelsemyndigheterna och för att skydda sitt eget liv och sin hälsa.

6 kap. **Utlämnande av underrättelseuppgifter i vissa fall**

I den militära underrättelseverksamheten är informationsinhämtningen vidsträckt och genom den inhämtas information om ett yttre, betydande hot som gäller Finland. Den allmänna behörigheten att förebygga, utreda och undersöka brott har polisen. Det främsta syftet med den militära underrättelseverksamheten är inte att inhämta information för att förebygga brott eller att inhämta information om förberedelse eller planering av brott.

Föremål för den militära underrättelseinhämtningen är verksamhet som inte nödvändigtvis är eller någonsin blir brottslig. Den militära underrättelseinhämtningen kan inriktas på att reda ut syftet med och bakgrunden till verksamhet som i sig är laglig, såsom ett fastighetsköp i närheten av vissa militära objekt.

Vidare ska militärunderrättelsemyndigheterna utplåna all överskottsinformation som inte anknyter till ett underrättelseuppdrag. Till följd av detta uppkommer det i den militära underrättelseinhämtningen i princip ingen information och inga upptagningar som kunde användas vid undersökning av brott, lämnande till åtalsprövning eller i en straffprocess.

Medan ett militärunderrättelseuppdrag pågår kan man råka i sådana situationer där den som utför ett underrättelseuppdrag oberoende av själva uppdraget upptäcker eller får kännedom om ett brott som har begåtts, som pågår eller planeras och som t.ex. var och en som omfattas av finsk jurisdiktion kan vara skyldig att anmäla. Eftersom den militära underrättelseinhämtningens lagenliga uppgift ska vara att inhämta information endast i ett visst i lagen noggrant avgränsat militärt syfte, ska anmälan av uppgifter för annan användning vara noggrant avgränsad och göras endast i situationer som överskrider en viss tröskel. I vissa situationer ska det således föreskrivas om en skyldighet för militärunderrättelsemyndigheterna att anmäla behövliga uppgifter som myndigheterna upptäckt till behörig förundersökningsmyndighet.

Syftet med kapitlets bestämmelser om överlåtelse av uppgifter om ett brott ska vara att trygga ändamålsbundenheten i fråga om uppgifter som erhållits med metoder för underrättelseinhämtning. Utgångspunkten är att de uppgifter som erhållits med metoder för underrättelseinhämtning inte ska få användas för annat syfte än för att utföra ett underrättelseuppdrag.

**76 §.** *Anmälan om en brottsmisstanke.* Enligt 1 mom. ska militärunderrättelsemyndigheterna utan oskäligt dröjsmål anmäla till centralkriminalpolisen, om det medan en metod för underrättelseinhämtning används framkommer att ett sådant brott kan antas ha begåtts för vilket det föreskrivna strängaste straffet är fängelse i minst sex år. I praktiken ska anmälan göras genast när det är möjligt. Om det finns ett ytterst viktigt och motiverat skäl till att skjuta upp anmälan, möjliggör bestämmelsen att anmälan skjuts upp med högst några dagar.

Uttrycket ”kan antas”, som gäller uppgiftens sannolikhet, ska göra tröskeln för att anmäla låg och uttrycket finns också som en förutsättning för att använda hemliga metoder för inhämtande av information i 5 kap. 2 § i polislagen. Militärunderrättelsemyndigheterna ska ansvara för att anmälan görs till centralkriminalpolisen. Centralkriminalpolisen ska i sin tur ansvara för att anmälan styrs vidare till den myndighet till vilken det hör att förrätta förundersökning eller vilken beslutar om förrättande av förundersökning. En förteckning över förundersökningsmyndigheterna finns i 2 kap. 1 § i förundersökningslagen (805/2011). Beslutet om att förrätta förundersökning i vissa situationer fattas av åklagaren. Till exempel när det är fråga om misstanke om att ett brott har begåtts i utlandet, förutsätter undersökning av det i Finland ett åtalsförordnande av riksåklagaren med stöd av 1 kap. 12 § i strafflagen (39/1889, ändr. 205/1997). I en dylik situation ska centralkriminalpolisen styra anmälan vidare till riksåklagarämbetet.

I första meningen i momentet ska för militärunderrättelsemyndigheterna ställas en skyldighet att anmäla brott för vilka det föreskrivna strängaste straffet är fängelse i minst sex år. Brott med en dylik påföljd präglas redan av ett så betydande intresse för att utreda brottet och intresse för att förverkliga straffansvaret att det med tanke på trovärdigheten hos straffrättssystemet är nödvändigt att anmäla dem till behörig myndighet, i detta fall centralkriminalpolisen. De brott som avses i paragrafen är bl.a. mord och människohandel. De brott som avses

ovan kan vad gäller intresset för att reda ut brottet och intresset för att förverkliga straffansvaret anses vara så stora att det i fråga om dem inte är acceptabelt att låta anmälan till förundersökningsmyndigheten vara beroende av prövning.

I praktiken ska anmälan göras genast när det är möjligt. Om det finns ett ytterst viktigt och motiverat skäl till att skjuta upp anmälan, möjliggör bestämmelsen att anmälan skjuts upp med högst några dagar. Bestämmelsen ställer ingen aktiv skyldighet för militärunderrättelsemyndigheterna att bland de uppgifter som erhållits med metoder för underrättelseinhämtning gallra ut uppgifter som är av betydelse med tanke på utredningen av ett brott, och detta uttrycks med ordet ”framkommer”.

Uttrycket ”kan antas” som gäller uppgiftens sannolikhet har motiverats med att det ska vara en låg förutsättning. I detta sammanhang kan det antas att ett brott har begåtts när en människa, som omsorgsfullt överväger sakernas tillstånd utifrån de uppgifter som föreligger, får en föraning om att ett brott har begåtts. Det ska dessutom finnas element av ett sådant brott för vilket det föreskrivna strängaste straffet är fängelse i minst sex år. Det ska inte vara fråga om en tröskel för att avslöja ett brott, eftersom det, såsom det sägs ovan, inte ska finnas någon aktiv skyldighet att gallra ut brottsinformation och därmed ska målet inte heller vara att reda ut om det föreligger en sådan grund för att inleda förundersökning som avses i 3 kap. 3 § 1 mom. i förundersökningslagen.

Militärunderrättelsemyndigheterna ska ansvara för att anmälan görs till centralkriminalpolisen. Centralkriminalpolisen ska i sin tur ansvara för att anmälan styrs vidare till den myndighet till vilken det hör att förrätta förundersökning eller vilken beslutar om förrättande av förundersökning. En förteckning över förundersökningsmyndigheterna finns i 2 kap. 1 § i förundersökningslagen. Beslutet om att förrätta förundersökning i vissa situationer fattas av åklagaren. Till exempel när det är fråga om misstanke om att ett brott har begåtts i utlandet, förutsätter undersökning av det i Finland ett åtalsförordnande av riksåklagaren med stöd av 1 kap. 12 § i strafflagen (39/1889, ändr. 205/1997). I en dylik situation ska centralkriminalpolisen styra anmälan vidare till riksåklagarämbetet.

Utöver anmälan ska militärunderrättelsemyndigheterna till centralkriminalpolisen också överlåta behövliga uppgifter om brottet. Hur behövliga de uppgifter är som ska överlåtas ska kunna bedömas först och främst ur den synvinkeln, vad som nödvändigtvis förutsätts för att förundersökning ska inledas. Överlåtelse av dylika uppgifter, såsom uppgifter om en händelse och parterna i den eller andra uppgifter som avses i 1 kap. 2 § 1 mom. i förundersökningslagen kommer naturligtvis i fråga endast i den omfattning som militärunderrättelsemyndigheterna har fått dylik information genom användning av en metod för underrättelseinhämtning. För det andra ska hur behövliga uppgifterna är kunna bedömas med tanke på bevisningen, och i samband med detta är det väsentliga information om sådana omständigheter som ska visas som stöd för ett straffyrkande som gäller ett misstänkt brott.

Enligt andra meningen i momentet ska anmälan genom beslut av Huvudstabens underrättelsechef få skjutas upp med högst ett år åt gången, om det är nödvändigt för att garantera försvaret av landet eller för att skydda den nationella säkerheten eller liv eller hälsa. Därmed ställs en hög tröskel, nödvändighet, för att skjuta upp anmälan. Anmälan ska få skjutas upp med högst ett år åt gången. Det ska dock vara möjligt att fatta flera beslut, om det varje gång kan presenteras adekvata grunder för detta.

Det första beslutet om uppskov ska fattas omedelbart, när det medan en metod för underrättelseinhämtning används framkommer sådan information om ett brott som avses i bestämmelsen.

Om det efter tidsfristen på ett år är befogat att förlänga uppskovstiden, ska ett nytt beslut fattas i god tid innan tidsfristen går ut. Om det blir tid över mellan den tidpunkt då tidsfristen går ut och den tidpunkt då ett nytt beslut fattas, är följden för det första att uppgiften utan oskäligt dröjsmål ska överlåtas till centralkriminalpolisen. För det andra kan föremålet för informationsinhämtningen under tiden mellan det beslut som förfallit och ett nytt beslut, åberopande en parts rätt till handling, få information om att en metod för underrättelseinhämtning har använts.

Det ska för det första vara möjligt att skjuta upp en anmälan, om det är nödvändigt för att trygga försvaret av landet eller skydda den nationella säkerheten. Tröskeln ”nödvändigt” ska vara hög och med den ska avses i sista hand, dvs. att försvaret av landet eller den nationella säkerheten i ett enskilt fall inte kan garanteras med andra metoder än att ett beslut fattas om att anmälan ska skjutas upp. Med motiveringen i fråga ska det kunna säkerställas att ett underrättelseuppdrag har kommit så långt att anmälan om det inte orsakar att t.ex. uppgifter om militärunderrättelsemyndigheternas taktiska eller tekniska metoder avslöjas, förutsatt att avslöjandet av dem skulle utgöra ett hot mot försvaret av landet eller den nationella säkerheten. Motiveringen till att en anmälan skjuts upp kan också sammanhänga med t.ex. behovet att undvika en förundersökning som oundvikligen inleds till följd av anmälan, och en skada för Finlands bilaterala relationer som blir följden av detta liksom också Finlands förutsättningar att agera i internationellt samarbete.

För det andra ska det vara möjligt att skjuta upp en anmälan, 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, varefter föremålet för underrättelseinhämtningen kan underrättas. Med motiveringen i fråga ska man också kunna säkerställa t.ex. att informationsinhämtningen kommit så långt att underrättelsen inte medför någon arbetssäkerhetsrisk.

Övriga kriterier för bedömning av om en anmälan kan skjutas upp ska ingå i 3 mom. Med beaktande av att militärunderrättelsemyndigheternas beslut om att skjuta upp en anmälan innebär ett undantag från den anmälningsskyldighet som är utgångspunkten, ska det vara motiverat att genast informera också underrättelseombudsmannen. En bestämmelse om detta finns i 105 §. När underrättelseombudsmannen har fått informationen ska ombudsmannen kunna göra en självständig bedömning av bl.a. om uppskovsbeslutet kan anses försvarbart i skenet av de kriterier som nämns i detta moment och i 4 mom. samt vid behov använda sin granskningsrätt för att övervaka uppskovsbeslutens laglighet.

Enligt 2 mom. ska militärunderrättelsemyndigheterna få anmäla ett begånget brott till centralkriminalpolisen, om det föreskrivna strängaste straffet för brottet är fängelse i minst tre år. I momentet ska det således ställas ett förbud mot överlåtelse av information som definieras i enlighet med en brottspåföljd på minst tre år när det gäller att reda ut ett brott. Uppgifter om sådana brott där det föreskrivna strängaste straffet underskrider tre år, ska alltid lämnas oanmälda vad gäller syftet att reda ut ett brott. Med beaktande av å ena sidan den anmälningsplikt, som det föreslås att det ska föreskrivas om i 1 mom., och å andra sidan det anmälningsförbud som beror på denna mening, ska det vara beroende av militärunderrättelsemyndigheternas prövning huruvida redan begångna brott med en påföljd på minst tre och högst tre år ska anmälas till centralkriminalpolisen eller inte. Beroendet av prövning ska dock vara bundet till de bedömningskriterier som nämns i 3 mom. I fråga om de behövliga uppgifter som gäller ett brott och som ska överlåtas i samband med anmälan hänvisas det till vad som konstateras ovan.

En anmälan som avses i 1 och 2 mom. ska inte inverka på fortgången av användningen av en metod för underrättelseinhämtning, om förutsättningarna för att använda metoden fortfarande föreligger. Verksamhet som är föremål för militär underrättelseinhämtning kan maskeras till kriminell verksamhet, och då måste man fortfarande kunna inhämta information om föremålen för underrättelseinhämtningen. Underrättelseverksamheten omintetgörs inte i och med att ett straffansvar realiseras.

I 3 mom. sägs det att när det övervägs om en anmälan ska skjutas upp enligt 1 mom. eller om en anmälan ska göras enligt 2 mom., ska betydelsen av utredningen eller förhindrandet av brottet med tanke på allmänna och enskilda intressen beaktas. I momentet ska de kriterier samlas genom vilka uppskjutandet av en anmälan och görandet av en anmälan som beror på prövning om ett redan begånget brott ska bedömas. Följaktligen ska militärunderrättelsemyndigheternas prövning i dessa åtgärder inte vara fri, utan bunden också till de bedömningskriterier som avses i 3 mom. Till följd av ändamålet med metoderna för underrättelseinhämtning är det klart att i de fall som gäller överlåtelse av information om ett brott som är beroende av prövning, är ett centralt bedömningskriterium överlåtelsens inverkan på försvaret av landet och på den nationella säkerheten. I en situation där en anmäla skjuts upp ska militärunderrättelsemyndigheterna emellertid i proportion till varandra ställa å ena sidan intresset att skydda försvaret av landet och den nationella säkerheten eller liv och hälsa och å andra sidan intresset att reda ut ett brott.

Enligt 1 mom. får Huvudstabens underrättelsechef skjuta upp en anmälan med högst ett år åt gången. För att Huvudstabens underrättelsechef faktiskt ska kunna bedöma vilken betydelse utredningen eller förhindrandet av ett brott har för allmänt och enskilt intresse, kan det i ett enskilt fall förutsätta en förfrågan hos centralkriminalpolisen eller den lokala polisen innan beslutet fattas. Med detta säkerställs det i fråga om de nämnda intressena att de så fullständigt som möjligt blir tryggade i den beslutsprövning som Huvudstabens underrättelsechef gör.

När det är fråga om att efter prövning göra en anmälan om ett redan begånget brott, bör man vid bedömningen koncentrera sig på hur anmälan betjänar utredningen av brottet med tanke på allmänt och enskilt intresse. Ju allvarligare brottsmisstanke det är frågan om, desto tyngre väger intresset att reda ut brottet med tanke på det allmänna intresset. Med tanke på det allmänna intresset bör det också beaktas huruvida det överhuvudtaget är möjligt att skjuta upp en anmälan eller göra en anmälan efter prövning om ett redan begånget brott utan en stor sannolikhet för att brottet förblir outrett. Utredningen av brottet äventyras åtminstone inte i ett sådant fall, om informationen i sig utgör ett väsentligt bevis för att gärningsmannen har gjort sig skyldig till ett brott. Med tanke på enskilt intresse är det igen av betydelse t.ex. om anmälan bedöms göra det möjligt att återbörda egendom som målsägande fått genom ett brott eller att verkställa förverkandepåföljd för den som dömts med anledning av ett brott eller skadestånd som tillkommer en målsägande.

Enligt 4 mom. ska en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman göra den anmälan som avses i paragrafen till centralkriminalpolisen. I de situationer som avses i paragrafen ska det vara fråga om ett redan begånget brott eller om misstanke om ett sådant. Till följd av detta vore det ändamålsenligt att uppgiften kunde anmälas till förundersökningsmyndigheten så snabbt som möjligt. Militärjurister och andra tjänstemän som är särskilt förtrogna med användningen av metoder för underrättelseinhämtning kan anses ha tillräckligt kunnande för att bedöma om det är frågan om ett redan begånget brott eller inte.

**77 §.** *Anmälan och lämnande av information i vissa fall*. Enligt 1 meningen i 1 mom. ska militärunderrättelsemyndigheterna utan dröjsmål anmäla till centralkriminalpolisen, 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.

I motsats till vad som är fallet i allmänhet, ska skyldigheten att anmäla ett brott som avses i bestämmelsen vara bunden till den anmälan som ska göras utan dröjsmål. Meningen i fråga ställer en betydligt strängare förpliktelse för militärunderrättelsemyndigheterna än för andra vad gäller reaktionstiden för att anmäla ett brott som avses i bestämmelsen. I praktiken ska en anmälan göras så snart som den mänskliga verksamheten och sättet att göra anmälan möjliggör.

Utgående från 2 mom. ska militärunderrättelsemyndigheterna få överlåta information till behöriga myndigheter om ett sådant brott som är på färde och ännu kan förhindras och som har framkommit medan en metod för underrättelseinhämtning användes, förutsatt att det straff som är påföljden för gärningen är fängelse i minst två år. För gärningar med en straffpåföljd som underskrider detta ska däremot gälla förbud mot överlåtelse av information. Med behörig myndighet ska utöver förundersökningsmyndigheterna avses t.ex. nödcentralen. Den information som ska överlåtas till behörig myndighet ska kunna anknyta förutom till förhindrande av brott, också till avslöjande av ett sådant eller t.ex. till utredning av tröskeln för att inleda en förundersökning. Bestämmelser om de kriterier som styr prövningen av informationsöverlåtelsen ska ingå i 3 mom. I fråga om de behövliga uppgifter som gäller ett brott och som ska överlåtas i samband med anmälan hänvisas det till vad som konstateras ovan i samband med 76 §. I samband med detta bör särskilt beaktas hot om brott som riktar sig mot liv och hälsa. Vidare kan det potentiella hot som vissa brott utgör för liv och hälsa tala för att anmälan bör göras. Till exempel ett betydande hot om våld som är kopplat till staten som institution och som riktas mot en person är en vägande grund för att göra en anmälan. Det kan vara fråga om en situation där det utgående från observationer av en persons beteende formas ett befogat antagande om en orättmätig attack, som riktas mot den person som avses ovan.

Det är klart att militärunderrättelsemyndigheterna trots anmälan får fortgå med den pågående informationsinhämtningen utgående från denna paragraf, om förutsättningarna för att använda metoden för underrättelseinhämtning fortfarande föreligger.

I 3 mom. ska det föreskrivas om den prövning som anknyter till anmälan. Till denna del kan det hänvisas till de omständigheter som nämns i 76 § 3 mom.

Enligt 4 mom. ska information som inhämtats genom användning av en metod för underrättelseinhämtning alltid få röjas som en utredning som stöder att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada.

Med tanke på jämlikhetsprincipen i förundersökningen samt den rätt till en rättvis rättegång och personlig frihet som tillkommer var och en är det klart att ju större risk en person löper att bli anhållen och häktad eller annars föremål för en straffrättslig påföljd på felaktiga grunder, desto allvarligare måste man förhålla sig till en begäran om en utredning som stöder att någon är oskyldig. Samma omständigheter måste man uppmärksamma på tjänstens vägnar också när militärunderrättelsemyndigheterna överväger att på eget initiativ anmäla en uppgift som stöder att någon är oskyldig. Militärunderrättelsemyndigheternas informationsöverlåtelse på eget initiativ som stöd för att någon är oskyldig kan komma i fråga närmast i situationer enligt 78 §,

dvs. då förundersökningsmyndigheten har meddelat militärunderrättelsemyndigheterna att förundersökning kommer att inledas, en förundersökningsåtgärd kommer att vidtas eller att en åtgärd som siktar till att förhindra ett brott kommer att inledas i fråga om en person som har varit eller fortfarande är föremål för informationsinhämtning. En begäran av en misstänkt om att få en utredning som stöd för att den misstänkte är oskyldig kommer i praktiken i fråga endast när personen har underrättats om att en metod för underrättelseinhämtning används.

En fara eller skada som avses i momentet behöver inte nödvändigtvis anknyta till ett brott eller ännu hålla på att utvecklas till ett brott, utan det kan vara fråga om t.ex. att förhindra en olycka eller om att förhindra en omfattande datanätsattack som riktar sig mot ett företag. Ju mera betydande faran för liv, hälsa eller frihet är, desto högre ska tröskeln vara att låta bli att göra en anmälan t.ex. till behörig myndighet. En anmälan ska också kunna göras till en enskild person eller sammanslutning, om detta behövs för att förhindra en betydande skada som räknas upp i momentet.

Enligt 5 mom. ska Huvudstabens underrättelsechef besluta om anmälan. Eftersom det i de situationer som avses i paragrafen är fråga om att förhindra ett brott, i fråga om vilket gränsdragningen mellan underrättelseverksamhet och brottsbekämpning i vissa situationer är beroende av tolkning, kan anmälan i vissa situationer äventyra underrättelseverksamheten eller en pågående brottsbekämpning. Huvudstabens underrättelsechef klarar bäst av att väga olika synpunkter mot varandra gällande anmälan till brottsbekämpningen.

Vidare kan Huvudstabens underrättelsechef i synnerhet i situationer enligt 3 mom. överväga hur det är ändamålsenligast att överlåta information t.ex. för att förhindra en ansenlig egendomsskada.

**78 §.** *Anmälan om att förundersökning eller brottsbekämpning inleds.* Enligt paragrafen ska, om en förundersökningsmyndighet utgående från en anmälan som avses i detta kapitel inleder en förundersökning eller vidtar en förundersökningsåtgärd eller om en brottsbekämpande myndighet inleder en åtgärd som syftar till att förhindra ett brott, förundersökningsmyndigheten eller den brottsbekämpande myndigheten innan förundersökning inleds, förundersökningsåtgärden vidtas eller en hemlig åtgärd för inhämtande av information vidtas till militärunderrättelsemyndigheterna anmäla detta. Syftet med paragrafen är att säkerställa att militärunderrättelsemyndigheterna fortsättningsvis har en lägesbild av, hurdana åtgärder förundersökningsmyndigheterna eller andra myndigheter har vidtagit utgående från den anmälan som militärunderrättelsemyndigheterna har gjort till dem.

Vidare ska det säkerställas att anmälan görs om användningen av en metod för underrättelseinhämtning i de situationer som avses i 86 § 7 mom. Enligt bestämmelsen ska den som varit föremål för en metod för underrättelseinhämtning underrättas om systematisk observation, förtäckt inhämtande av information, en täckoperation, bevisprovokation genom köp, styrd användning av informationskällor och platsspecifik underrättelseinhämtning, om förundersökning har inletts i ärendet. I 3 kap. 3 § i förundersökningslagen föreskrivs om inledande av förundersökning. Med en förundersökningsåtgärd avses bl.a. förhör och konfrontation. Åtgärder som syftar till att förhindra ett brott är bl.a. gripande av en person, tillträde till en lokal som skyddas av hemfrid eller offentlig frid och isolering av en plats och ett område.

## 7 kap. Förbud mot underrättelseinhämtning, utplåning av underrättelseinformation och underrättelse om användning av en metod för underrättelseinhämtning

**79 §.** *Förbud mot underrättelseinhämtning.* Enligt 1 mom. får teleavlyssning, observation på teknisk väg eller underrättelseinhämtning som avser datatrafik inte riktas mot sådan kommunikation eller ett sådant meddelande, 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 sägs att ett rättegångsbiträde eller ett rättegångsombud 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. Vidare föreskrivs det i paragrafen att en advokat, ett rättegångsbiträde som avses i lagen om rättegångsbiträden med tillstånd eller ett offentligt rättsbiträde inte olovligen får 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.

En person som är väsentlig med tanke på ett underrättelseuppdrag kan ha att göra med ett rättegångsbiträde också i ett annat sammanhang än i ställningen som misstänkt för ett brott. Det kan vara fråga om en situation där en person som är väsentlig med tanke på ett underrättelseuppdrag i samband med användningen av metoder för underrättelseinhämtning vid militär underrättelseinhämtning går igenom uppgifter som anknyter till en skilsmässa eller ett testamente, varvid situationen enligt EIT:s tolkningspraxis har bedömts som ett ingrepp i integritetsskyddet.

I båda fallen ovan är en förutsättning att en viss jurist är rättegångsbiträde för en person som är viktig med tanke på ett underrättelseuppdrag och en dylik relation har uppkommit. För att det ska kunna verifieras att en relation har uppkommit, måste militärunderrättelsemyndigheterna under någon tid följa med parternas kommunikation. Genast när en sådan relation har verifierats, ska militärunderrättelsemyndigheterna utplåna all den information som omfattas av förbud mot underrättelseinhämtning.

I 17 kap. 14 § i rättegångsbalken sägs 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 sägs att en präst och en 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.

I 17 kap. 20 § i rättegångsbalken föreskrivs att när ett meddelande enligt lagen om yttrandefrihet i masskommunikation har gjorts tillgängligt för allmänheten, får meddelandets upphovsman, utgivaren och utövaren av programverksamheten vägra vittna om vem som har lämnat de upplysningar som meddelandet grundar sig på samt om upphovsmannens identitet.

Rättegångsbalkens 17 kap. 22 § 2 mom. breddar det personliga tillämpningsområdet för vissa av de ovan nämnda förbuden att vittna och rättigheterna att vägra vittna. Enligt bestämmelsen i fråga 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. Den hänvisning till 11 § 2 och 3 mom. som ingår i 22 §

2 mom. i rättegångsbalken är inte tillämplig här, eftersom det inte annars heller föreslås att det ska föreskrivas om ett uttryckligt avlyssnings- och observationsförbud som anknyter till 11 § i rättegångsbalken.

Den metod för underrättelseinhämtning som avses i 1 mom. ska inte heller få installeras för att användas på en sådan plats där det kan antas att en uppgift som avses i 1 mom. och i fråga om vilken gäller skyldighet eller rätt att vägra vittna som avses i momentet kan bli föremål för underrättelseinhämtning och skyldigheten eller rätten att vägra vittna åtnjuter skydd för de grundläggande fri- och rättigheterna enligt Finlands grundlag. Sådana platser är t.ex. läkarmottagningar, advokatbyråer, juridiska byråer, mediehus och tidningsredaktioner, utrymmen som används av en präst i ett sådant registrerat religionssamfund som avses i religionsfrihetslagen (453/2003) och servercenter som kan antas förmedla i paragrafen avsedd information som omfattas av tystnadsplikt eller tystnadsrätt.

I samtliga fall i 1 mom. ska betydelse ges relationen mellan en person som är föremål för militär underrättelseinhämtning och en person som omfattas av förbud mot underrättelseinhämtning samt det att den person som omfattas av förbud mot underrättelseinhämtning faktiskt uppfyller de krav som ställts i fråga om förbudet mot underrättelseinhämtning.

I 2 mom. anges att åtgärden ska avbrytas och de upptagningar som fåtts genom den och anteckningarna om de uppgifter som fåtts genom den genast utplånas, om det under tiden 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.

Skyldigheten att genast utplåna uppgifterna kompletterar iakttagandet av avlyssnings- och observationsförbudet. Om det vid informationsinhämtandet visar sig att förbudet att inrikta metoder för underrättelseinhämtning, vilket avses i första momentet, har överträtts, ska den skyldighet att utplåna upptagningar och anteckningar som ställs i 2 mom. genast iakttas när det har kommit fram att kommunikationen omfattas av förbud mot underrättelseinhämtning. En sådan situation kan det bli fråga om t.ex. när personers namn och roller inte ännu är klara medan kommunikationen pågår eller när t.ex. kommunikationen inte avlyssnas i realtid.

Enligt 3 mom. ska förbudet mot underrättelseinhämtning 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.

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 att 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.

I 4 mom. ska det föreskrivas att de förbud mot underrättelseinhämtning som avses i denna paragraf dock inte gäller sådana fall där en i 1 mom. avsedd person är föremål för användning av en metod för underrättelseinhämtning på samma grund som en person som står i kontakt med den person som avses i 1 mom. och beslut om teleavlyssning, inhämtande av information i stället för teleavlyssning, optisk observation eller underrättelseinhämtning som avser datatrafik har fattats även om denna person.

Att vara föremål ska täcka situationer där en person som avses i 1 mom. och en person som är viktig med tanke på ett underrättelseuppdrag bedriver samarbete som är betydande med tanke på den militära underrättelseinhämtningen. Enbart ett samarbete mellan två personer räcker ännu inte för att man ska kunna låta bli att följa förbudet, utan i fråga om båda personerna ska det finnas ett beslut om användning av samma metod för underrättelseinhämtning. Båda personerna ska således vara föremål för ett underrättelseuppdrag och information om deras förehavanden ska kunna inhämtas med samma befogenhet.

**80 §.** *Kopieringsförbud.* I paragrafen ska det föreskrivas om kopieringsförbud. I samband med militär underrättelseinhämtning ska det observeras att utgångspunkten är att den information som inhämtats med metoder för underrättelseinhämtning inte är avsedd att användas som bevis i en straffprocess. Kopieringsförbud har inte samma betydelse i underrättelseverksamhet som när straffprocessuella befogenheter utövas. Det är inte heller möjligt att tillämpa kopieringsförbud enhetligt med motsvarande bestämmelser om förbud mot tagande i beslag och kopiering samt bevisning.

Enligt 1 mom. ska handlingar eller andra objekt som avses i 1 mom. inte få kopieras, om de 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.

Bestämmelsen motsvarar till denna del de kopieringsförbud om vilka föreskrivs i 7 kap. 3 § 1 mom. i tvångsmedelslagen.

Enligt 2 mom. är, om sekretessen, tystnadsplikten eller tystnadsrätten grundar sig på 17 kap. 11 § 2 eller 3 mom. i rättegångsbalken eller 13, 14, 16 eller 20 § i det kapitlet, 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., eller av den till vars förmån tystnadsplikten eller tystnadsrätten har föreskrivits.

Bestämmelsen motsvarar till denna del de kopieringsförbud om vilka föreskrivs i 7 kap. 3 § 2 mom. i tvångsmedelslagen. Förbudet gäller endast när handlingen innehas av en person som nämns i momentet eller av den till vars förmån tystnadsplikten har föreskrivits. Innehas ska tolkas på motsvarande sätt som i gällande lagstiftning. Innehavandet omfattar sålunda också en försändelse som transporteras av posten, en kurir eller en annan tredje part. Till följd av underrättelseverksamhetens art kommer denna bestämmelse inte att tillämpas ofta.

Enligt 3 mom. gäller kopieringsförbud 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, eller 2) i 17 kap. 20 § 1 mom. i rättegångsbalken avsedd person samtycker till kopiering.

Bestämmelsen motsvarar de kopieringsförbud om vilka föreskrivs i 7 kap. 3 § 3 mom. i tvångsmedelslagen. Till följd av underrättelseverksamhetens art kommer denna bestämmelse inte att tillämpas ofta.

Enligt 4 mom. får handlingar eller data som innehas av ett teleföretag eller en sammanslutningsabonnent och som innehåller uppgifter om meddelanden som avses i 32 § 1 mom. eller innehåller identifieringsuppgifter som avses i 35 § 1 mom. eller basstationsuppgifter som avses i 37 § 1 mom. inte kopieras. Genom detta omnämnande i momentet förhindras att de befogenheter som avses ovan kringgås.

**81 §.** *Utplåning av underrättelseinformation*. Enligt 1 mom. ska information som erhållits med en metod för underrättelseinhämtning utplånas utan dröjsmål efter att det har framgått att informationen inte behövs för skötsel av uppdrag inom den militära underrättelseinhämtningen eller att informationen inte behövs med avseende på landets försvar eller för att skydda den nationella säkerheten.

Momentet gäller all slags information som fåtts med en metod för underrättelseinhämtning. Ganska snart blir det redan till följd av informationens art klart om den behövs för att trygga försvaret av landet eller skydda den nationella säkerheten eller om den kan utplånas.

Enligt 2 mom. ska de basstationsuppgifter som avses i 37 § utplånas när det har framgått att informationen inte behövs för skötsel av uppdrag inom den militära underrättelseinhämtningen eller att informationen inte behövs med avseende på landets försvar eller för att skydda den nationella säkerheten. Bestämmelsen motsvarar 5 kap. 55 § 3 mom. i gällande polislag med den skillnaden att i detta moment sammanhänger behovet av information med skötseln av uppdrag inom den militära underrättelseinhämtningen eller med tryggandet av landets försvar eller skyddandet av den nationella säkerheten.

Enligt 3 mom. ska en kopia som avses i 54 och 55 § utplånas utan dröjsmål, om det framgår att kopieringen har riktats mot material som omfattas av kopieringsförbud eller att informationen inte behövs med tanke på landets försvar eller för att skydda den nationella säkerheten.

Enligt 4 mom. ska information dock få bevaras och lagras, om den behövs i fall som anges i 76 eller 77 §. Information som inte ska utplånas ska bevaras i fem år efter det att saken har avgjorts genom en lagakraftvunnen dom eller avskrivits.

Information som har erhållits med en metod för underrättelseinhämtning och som inte anknyter till tryggandet av landets försvar eller skyddandet av den nationella säkerheten ska i princip utplånas. Då kan man också utplåna material som behövs för att förhindra ett grovt brott eller

som stöd för att en misstänkt är oskyldig. På grund av detta är det nödvändigt att tillåta att undantag görs från huvudregeln, så att material som behövs för att förhindra ett grovt brott samt som stöder att någon är oskyldig vid behov ska kunna användas vid en rättegång.

**82 §.** *Avbrytande av teleavlyssning, teknisk avlyssning, radiosignalspaning, teknisk observation av utrustning och platsspecifik underrättelseinhämtning*. Enligt 1 mom. ska om det framgår att teleavlyssningen riktas mot något annat meddelande än ett meddelande från eller till den som är föremål för tillståndet eller att den person som den tekniska avlyssningen riktas mot inte befinner sig i det utrymme eller på den plats som avlyssnas, avlyssningen avbrytas så snart som möjligt och de upptagningar som fåtts genom avlyssningen och anteckningarna om de uppgifter som fåtts genom den genast utplånas.

Betydelsen av bestämmelsen framhävs framför allt i fråga om teleavlyssning som riktas mot en person. Vid teleavlyssning som riktas mot en person är föremålet för användningen av en metod för underrättelseinhämtning de teleterminalutrustningar och teleadresser som personen använder. Medan en metod för underrättelseinhämtning används kan personen t.ex. sälja eller ge vidare en teleterminalutrustning som personen använder, varvid teleavlyssning kan komma att rikta sig mot teleterminalutrustningens senare användare.

I 2 mom. ska det föreskrivas om särskilda skyldigheter till omedelbar utplåning gällande teknisk observation av utrustning och radiosignalspaning. Enligt den föreslagna bestämmelsen i 58 § 3 mom. som gäller radiosignalspaning får man genom radiosignalspaning inte inhämta information om innehållet i ett meddelande från någon annan än en statlig aktör. Till följd av radiosignalspaningens art kan föremål för den bli kommunikation som åtnjuter skydd för hemligheten i fråga om ett förtroligt meddelande. Enligt det moment som behandlas här ska ett sådant meddelande och anteckningar om det genast utplånas. Med avbrytande ska i detta fall inte avses att all radiosignalspaning avbryts utan radiosignalspaningen ska till denna del inriktas på nytt så att kommunikation till och från någon annan än en statlig aktör inte längre blir föremål för radiosignalspaning.

Enligt den bestämmelse som föreslås i 30 § 2 mom. och som gäller teknisk observation av utrustning ska med teknisk observation av utrustning inte få inhämtas information om en annan persons meddelande än den som är föremål för observationen eller om innehållet i ett meddelande som förmedlas och inte heller om dess identifieringsuppgifter. På motsvarande sätt som i fråga om teleavlyssning, som behandlas i 1 mom. i denna paragraf, ska man utplåna innehållet i och identifieringsuppgifterna till ett meddelande till eller från någon annan än en person som är föremål för observation i överensstämmelse med tillståndet eller meddelanden som förmedlas.

I paragrafens 3 mom. ska det på motsvarande sätt som i 81 § 4 mom. föreskrivas om användning av den information som samlats fram till dess metoden för underrättelseinhämtning avbryts. Informationen kan anknyta till en brottsmisstanke, om vilken föreskrivs i 76 § eller till brottsbekämpning, om vilken föreskrivs i 77 §, och denna information ska kunna utnyttjas på de sätt som avses i bestämmelserna.

**83 §.** *Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik*. I paragrafen ska det föreskrivas om särskilda skyldigheter till utplåning gällande underrättelseinhämtning som avser datatrafik.

I fråga om de uppgifter som inhämtats genom underrättelseinhämtning som avser datatrafik ska gälla skyldigheten att utplåna underrättelseinformation, om vilken föreskrivs i 81 §, men

till följd av den särskilda karaktären hos underrättelseinhämtning som avser datatrafik ska dessutom finnas vissa särskilda utplåningsskyldigheter, vilka sammanhänger med informationens speciella karaktär. Utplåningsskyldigheten ska å enda sidan gälla uppgifter som omfattas av förbud mot underrättelseinhämtning. Skyldigheten att utplåna uppgifter som omfattas av förbudet mot underrättelseinhämtning och det därav följande förbudet att utnyttja dem på något som helst sätt är ovillkorliga och det är inte tillåtet att avvika från dem. Skyldigheten att utplåna oväsentliga uppgifter är däremot inte ovillkorlig, utan från den är det möjligt att avvika i situationer som specificeras i 76 eller 77 § eller i sådana situationer om vilka föreskrivs i 85 §.

Enligt 1 punkten i momentet ska information som erhållits genom underrättelseinhämtning som avser datatrafik utplånas utan dröjsmål, om det framgår att båda parterna i kommunikationen befann sig i Finland när kommunikationen försiggick. Skyldigheten ska kompletteras med ett förbud mot underrättelseinhämtning, om vilket ska föreskrivas i den föreslagna bestämmelsen i 79 § 3 mom. Enligt nämnda paragraf ska underrättelseinhämtning som avser datatrafik inte få inriktas på ett meddelande, vars avsändare och mottagare befinner sig i Finland (s.k. inhemskt meddelande). Till den del som dylika meddelanden, som omfattas av förbud mot underrättelseinhämtning, trots allt filtreras ut för behandling, ska de med stöd av bestämmelsen i fråga utplånas utan dröjsmål, när deras karaktär av inhemska meddelanden har framgått.

Den praktiska betydelsen av utplåningsskyldigheten framhävs av att det tekniskt inte är möjligt att fullständigt följa det förbud mot underrättelseinhämtning som gäller inhemsk kommunikation enligt 79 § 3 mom. Ett meddelande kan dirigeras till mottagaren via utlandet, dvs. så att det överskrider Finlands gräns, även om både meddelandets avsändare och mottagare de facto befinner sig i Finland. Genom utformningen av de sökbegrepp som ska användas vid det automatiserade avskiljandet inom datatrafiken kan man i någon mån minska risken för att dylika inhemska meddelanden ingår i det insamlade materialet. Risken kan dock i allmänhet inte avlägsnas helt, vilket gör att också inhemska meddelanden kan bli föremål för manuell behandling i den underrättelseinhämtning som avser datatrafik. Vid den manuella behandlingen kan ett meddelandes inhemska karaktär framgå redan när meddelandets styr- och förmedlingsuppgifter granskas, och i ett sådant fall ska meddelandet utplånas utan dröjsmål utan att innehållet i det reds ut. I en del fall kan man upptäcka ett meddelandes inhemska karaktär först när dess innehåll reds ut manuellt, varvid utredningen av innehållet omedelbart ska avslutas och meddelandet utan dröjsmål utplånas.

Enligt 2 punkten i momentet ska information, som erhållits genom underrättelseinhämtning som avser datatrafik och i fråga om vilken avsändaren eller mottagaren eller lagraren har skyldighet eller rätt att vägra vittna på det sätt som avses i 79 § 1 mom., genast utplånas. Utplåningsskyldigheten ska i överensstämmelse med hänvisningen i 79 § 1 mom. gälla uppgifter som avses i 17 kap. 13, 14, 16 och 20 § samt 22 § 2 mom. i rättegångsbalken och om vilka de yrkespersoner som avses i bestämmelserna i fråga är skyldiga eller har rätt att vägra vittna om. Utplåningsskyldigheten ska inte gälla all kommunikation från yrkespersonerna i fråga, utan utplåningsskyldigheten ska avgöras av innehållet i uppgiften. Också om skyldighet att utplåna en uppgift som ingår i en yrkespersons kommunikation inte föreligger enligt denna punkt, kan skyldighet föreligga enligt 1 punkten i momentet.

I bestämmelsen ska utöver en uppgifts avsändare och mottagare, dvs. parterna i en två- eller flervägskommunikation, också särskilt nämnas den som lagrar uppgiften. Med den som lagrar en uppgift ska avses den person som lagrar data, t.ex. ett dokument, i en molntjänst. Om inne-

hållet i ett sådant dokument som ska lagras i en molntjänst omfattas av ett förbud att vittna eller en rätt att vägra vittna, vilka avses i bestämmelsen, ska dokumentet utplånas.

Uppgiften ska utplånas utan dröjsmål när det har framgått att den omfattas av ett förbud mot underrättelseinhämtning som anknyter till rättegångsbalken. Av de orsaker som refereras i detaljmotiveringen till 79 § 3 mom. kan det hända att saken upptäcks först i samband med att innehållet i ett meddelande reds ut. Med skyldigheten att omedelbart förstöra uppgifterna ska i dessa situationer avses att en närmare utredning av innehållet i en uppgift som omfattas av förbudet att vittna eller rätten att vägra vittna omedelbart ska upphöra och att uppgifterna och eventuella anteckningar om dem omedelbart ska förstöras.

Enligt 2 mom. ska militärunderrättelsemyndigheterna svara för utplåningen av uppgifterna. I första hand ska den militärunderrättelsemyndighet som använder en metod för underrättelseinhämtning svara för att uppgifterna utplånas med stöd av den bestämmelse som gäller granskning av upptagningar, om vilken ska föreskriva i 107 §. När ett underrättelseuppdrag genomförs kan uppgifter som erhållits genom underrättelseinhämtning som avser datatrafik, som använts som en del av uppdraget, komma att överföras också till Huvudstaben från Försvarsmaktens underrättelsetjänst, och med anledning av detta ska också Huvudstaben ha skyldighet att granska de uppgifter som inhämtats med underrättelseinhämtning som avser datatrafik på så sätt att den utplåningsskyldighet som avses i denna paragraf förverkligas.

Enligt andra meningen i momentet svarar Försvarsmaktens underrättelsetjänst för att uppgifterna utplånas, om inhämtandet av uppgifter i datatrafiken grundar sig på ett tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning. Militärunderrättelsemyndigheterna ska inte ha möjlighet eller befogenhet att behandla uppgifter som inhämtats genom tekniskt genomförande av underrättelseinhämtning som avser datatrafik, vilket gör att det är naturligt att Försvarsmaktens underrättelsetjänst, som är den tekniska genomföraren, ska svara för utplåningen av uppgifterna till den del som de inte svarar mot de sökbegrepp eller kategorier av sökbegrepp som har definierats i det tillstånd som skyddspolisen har ansökt om hos domstolen. Efter att uppgifterna har överlåtits till skyddspolisen, svarar skyddspolisen för utplåningen.

De skyldigheter att genast utplåna uppgifter som nämns i paragrafen är det inte möjligt att realisera på det stadium då filtrering görs i datatrafiken. Till följd av detta är det naturligt att då datatrafik vid den fortsatta behandlingen behandlas automatiskt och manuellt, ska det material raderas som har identifierats som sådant som omfattas av skyldigheten till omedelbar utplåning. I första hand ska Försvarsmaktens underrättelsetjänst, som är den som genomför militärunderrättelsemyndigheternas underrättelseinhämtning som avser datatrafik, svara för detta. I en del fall kan det dock uppkomma en situation där Huvudstaben, som är en militärunderrättelsemyndighet, i sin egen behandling upptäcker information som omfattas av skyldigheten till omedelbar utplåning, varvid Huvudstaben svarar för att informationen utplånas.

I sådana situationer där underrättelseinhämtning som avser datatrafik har genomförts för skyddspolisens räkning, är det naturligt att skyddspolisen svarar för att informationen utplånas. Vid tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning fortgår inte behandlingen vid militärunderrättelsemyndigheten av datatrafik som inhämtats för skyddspolisens räkning i enlighet med det tillstånd som skyddspolisen skaffat, utan datatrafiken överlåts till skyddspolisen för fortsatt behandling. Sålunda har Försvarsmaktens underrättelsetjänst, som är teknisk genomförare, inte möjligheter att fördjupa sig i den inhämtade datatrafiken och sålunda inte heller möjligheter att identifiera material som omfattas av skyldigheten till omedelbar utplåning.

I paragrafens 3 mom. ska det föreskrivas på motsvarande sätt som i 81 § 4 mom. om användning av den information som avses i paragrafen för att reda ut brott och för brottsbekämpning.

**84 §.** *Avslutande av användningen av en metod för underrättelseinhämtning om vilken beslut har fattats i en brådskande situation och utplåning av uppgifter som erhållits genom den*. I paragrafen ska det föreskrivas om utplåning av uppgifter som erhållits i situationer som avses i 25, 27, 29, 31, 36, 38, 53, 57, 66 eller 68 § i lagen där beslut i en brådskande situation har fattats av Huvudstabens underrättelsechef, en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller en annan tjänsteman, om domstolen eller en annan beslutsfattare anser att det inte fanns några förutsättningar för att inleda användningen av metoden för underrättelseinhämtning. Användningen av metoden för underrättelseinhämtning ska avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt ska genast utplånas.

Ett negativt beslut som domstolen har avgett efter ett beslut i en brådskande situation, ska meddelas till underrättelseombudsmannen för undersökning av om förfarandet med beslutet i en brådskande situation var lagenligt. I fråga om den information som erhållits genom ett beslut i en brådskande situation är det i princip fråga om lagligt erhållen information. Ifall domstolen i efterhand anser att det inte fanns några grunder för beslutet i en brådskande situation, kan detta beroende på hur allvarligt det eventuella felaktiga förfarandet är leda till en situation där den information som erhållits med metoden för underrättelseinhämtning inte kan utnyttjas som en utredning som stöder att någon är skyldig eller som bevisning som visar att någon är skyldig. Domstolen kan, när den avger ett negativt beslut, också uttala sig om hur användbara de uppgifter är som erhållits i ett förfarande med ett beslut i en brådskande situation för att reda ut ett brott med beaktande av hur allvarlig den rättskränkning är som anknyter till sättet att inhämta uppgifterna. En allmän utgångspunkt vid övervägningen kan då anses vara å ena sidan intresset av att reda ut saken (brottets allvar) som en synpunkt som talar för att bevisen ska utnyttjas och å andra sidan de negativa konsekvenserna av att bevisen utnyttjas som en synpunkt som talar för ett förbud. Utnyttjandet kan å ena sidan kränka den misstänktes rättsskydd och å andra sidan vara till hjälp i att hitta den materiella sanningen samt tjäna realiserandet av målsägandes rättigheter. Som en allmän utgångspunkt ska det också kunna anses att information som erhållits med ett beslut i en brådskande situation ska kunna utnyttjas för att stöda att den åtalade är oskyldig.

I 2 mom. ska det föreskrivas om utplåning av information som erhållits genom kopiering i en brådskande situation. Det ska vara fråga om en situation i analogi med det som sägs i 1 mom. Om en tjänsteman vid en militärunderrättelsemyndighet i brådskande ordning har beslutat om kopiering, men en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman anser att det inte har funnits förutsättningar för åtgärden, ska det material som fåtts genom kopieringen och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas.

Enligt 3 mom. ska de uppgifter som avses i paragrafen och som erhållits i en brådskande situation fram till dess förfarandet avbryts dock få användas under samma förutsättningar som uppgifterna får användas enligt 76 eller 77 §.

**85 §.** *Användning av en uppgift som inte anknyter till ett underrättelseuppdrag.* I 1 mom. ska det föreskrivas om användning av en uppgift som inte anknyter till ett underrättelseuppdrag vid utförandet av ett annat pågående eller kommande underrättelseuppdrag. En dylik uppgift ska kunna användas i situationer där uppgiften hade fått inhämtas med samma metod för underrättelseinhämtning som den uppgift som inte anknyter till underrättelseuppdraget fick

inhämtas med. Om den inhämtade uppgiften har inhämtats med en metod för underrättelseinhämtning som förutsätter tillstånd av domstol, ska användningen av uppgiften förutsätta prövning av domstolen.

Vid utförandet av ett underrättelseuppdrag kan det medan metoder för underrättelseinhämtning används komma en uppgift som inte är relevant för det pågående underrättelseuppdraget. I en situation kan det vara fråga om t.ex. ett underrättelseuppdrag, vars syfte är att bevaka en viss militär övning i utlandet, men i samband med den erhålls information om en underrättelseinsats som riktas mot landets försvar.

En uppgift som inte anknyter till ett underrättelseuppdrag ska få användas i ett annat underrättelseuppdrag, om samma metod för underrättelseinhämtning hade fått användas i det andra underrättelseuppdraget. Beslutet om att använda en uppgift som inte anknyter till ett underrättelseuppdrag ska alltid fattas av den part som skulle få fatta beslut om användning av metoden för underrättelseinhämtning i situationen i fråga. Om den inhämtade uppgiften t.ex. hade inhämtats med en metod för underrättelseinhämtning för vilken förutsätts tillstånd av domstol, ska en sådan uppgift kunna användas endast med tillstånd av domstolen.

Vid bevarandet av en uppgift som inte anknyter till ett underrättelseuppdrag ska de bestämmelser som gäller utplåning av uppgiften och behandling av personuppgifter alltid beaktas. En bedömning ska alltid göras när de upptagningar och handlingar som har uppkommit i samband med användningen av en metod för underrättelseinhämtning granskas, om vilken föreskrivs i 107 § i denna lag.

I 2 mom. ska det föreskrivas om användning i en brådskande situation av en uppgift som inte anknyter till ett underrättelseuppdrag. Förfarandet med beslut i en brådskande situation ska motsvara det som föreskrivs om annat förfarande med beslut i en brådskande situation. Enligt momentet ska en för uppdraget förordnad med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman få besluta om användningen av en uppgift som inte anknyter till ett underrättelseuppdrag till dess den part som beslutar om användning av en metod för underrättelseinhämtning har avgjort yrkandet om användning av uppgiften.

I ett förfarande med beslut i en brådskande situation ska ärendet ges till den beslutsfattare som avses i 1 mom. för avgörande genast när det är möjligt, dock senast 24 timmar efter det att metoden för underrättelseinhämtning började användas.

Det är klart att en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman inte ska kunna avgöra ett yrkande som personen själv har ställt. I dessa situationer ska beslutet naturligtvis fattas av någon annan som uppfyller samma krav. Redan förvaltningslagen förutsätter detta.

I 3 mom. ska det föreskrivas i informativt syfte om den uppgift som kan användas i situationer enligt 76 eller 77 §. I de bestämmelser som det hänvisas till är det fråga om en uppgift som inte anknyter till utförandet av ett underrättelseuppdrag. Medan ett underrättelseuppdrag utförs kan det emellertid komma emot sådana situationer där ett brott har begåtts eller där det visar sig att någon med sannolikhet kommer att göra sig skyldig till ett brott. Dessa är uppgifter som måste bedömas med stöd av skyldigheten och rätten att anmäla enligt 76 eller 77 §.

**86 §.** *Underrättelse om användning av en metod för underrättelseinhämtning.* Enligt första meningen i paragrafens 1 mom. ska den person som varit föremål för teleavlyssning, inhäm-

tande av information i stället för teleavlyssning, teleövervakning och teknisk observation samt kopiering som riktas mot ett meddelande eller sådan kopiering av en försändelse som riktas mot ett meddelande utan dröjsmål underrättas om detta skriftligen efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts.

I det föreslagna momentet räknas de metoder för underrättelseinhämtning upp som föremålet för en åtgärd ska underrättas om. Det ska vara fråga om sådana metoder för underrättelseinhämtning genom vilka det ingrips i skyddet för hemligheten i fråga om ett förtroligt meddelande i fråga om den person som är föremål för användningen av en metod för underrättelseinhämtning. I paragrafen ska den i momentet avsedda skyldigheten att underrätta föremålet för underrättelseinhämtning om användningen av en metod för underrättelseinhämtning i princip kopplas till den tidpunkt då informationsinhämtningen har avslutats. En underrättelse som avges efter denna tidpunkt äventyrar inte pågående informationsinhämtning. Informationsinhämtningen har kunnat avslutas antingen för att syftet med den har uppnåtts eller för att informationsinhämtningen har visat sig vara resultatlös.

Underrättelsen ska vara preciserad på ett sådant sätt att föremålet vid behov kan ta reda på orsaken till att en metod för underrättelseinhämtning har använts mot personen. I underrättelsen ska nämnas t.ex. vilken metod för underrättelseinhämtning som använts samt var och när den använts. Taktiska och tekniska detaljer om informationsinhämtningen behöver myndigheten dock inte avslöja. Underrättelsen till föremålet ska kunna göras t.ex. per brev till dennes senast kända adress. Andra personer än föremålet för informationsinhämtningen behöver inte underrättas om användning av en metod för underrättelseinhämtning, även om dessa de facto blivit utsatta för åtgärden. Underrättelseskyldigheten ska således omfatta endast de personer som de facto är föremål för informationsinhämtning, dvs. de personer i fråga om vilka ett yrkande har ställts eller ett beslut har fattats om användning av en metod för underrättelseinhämtning.

När användningen av en metod för underrättelseinhämtning faktiskt har avslutats innan tillståndets eller beslutets giltighetstid löper ut, och något nytt tillstånd inte har sökts eller förlängning av beslutet gjorts, ska underrättelsen till föremålet ges vid den faktiska avslutningstidpunkten. Om informationsinhämtningen fortgår med stöd av ett nytt tillstånd eller beslut om förlängning, ska underrättelsen ges antingen när användningen av en metod för underrättelseinhämtning faktiskt avslutas eller när tillståndets eller beslutets giltighetstid löper ut. Med tanke på informationsinhämtningens kontinuitet kan några dagars avbrott mellan beslutens giltighet godtas. Således ska föremålet utan dröjsmål underrättas om att en metod för underrättelseinhämtning har använts efter att en pågående eller kommande underrättelseinsats inte längre behöver tryggas.

I paragrafens 2 mom. föreskrivs det att andra än statliga aktörer ska underrättas om att underrättelseinhämtning som avser datatrafik har använts. På det sätt som framgår av den allmänna motiveringen har Europeiska domstolen för de mänskliga rättigheterna i många av sina avgöranden tagit ställning till frågan om huruvida en person som är föremål för informationsinhämtning bör och i vilka situationer i så fall ha rätt att av myndigheten få kännedom om en informationsinhämtningsåtgärd som har inriktats på personen. Europadomstolen har i sin avgörandepraxis betonat att den person som är föremål för informationsinhämtning måste kunna anföra besvär eller klagomål om informationsinhämtningsåtgärden. En förutsättning för att använda besvärs- eller klagomålsmöjligheten är i allmänhet att personen av myndigheten blir underrättad om informationsinhämtning som riktats mot honom eller henne efter att användningen av metoden för informationsinhämtning har avslutats. Av Europadomstolens avgörandepraxis följer emellertid inte att underrättelsen måste göras omedelbart efter att informationsinhämtningen har avslutats. Ett hot, som man har inhämtat information om med hjälp av en

metod för underrättelseinhämtning, kan fortgå i åratal eller till och med i decennier, varvid det är nödvändigt att skjuta upp underrättelsen i motsvarande grad för att skydda säkerhetsmyndigheternas verksamhet. För att möjliggöra användning av ett rättsmedel ska underrättelsen dock göras efter att det inte längre finns någon individuell grund för att avstå från underrättelsen. Ett system som inte förutsätter att den person som är föremål för en åtgärd underrättas kan emellertid också stå i samklang med människorättsfördraget. Härvid bör rätten att anföra klagomål ha tagits in i den nationella lagstiftningen på en så allmän nivå att vem som helst kan anföra klagomål enbart på den grunden att personen misstänker att myndigheterna har ingripit i det skydd som personens förtroliga kommunikation åtnjuter (Kennedy v. Förenade Konungariket). I den föreslagna paragrafen ska skyldigheten att underrätta en person om underrättelseinhämtning som avser datatrafik avgränsas till sådana fall, där underrättelseinhämtning som avser datatrafik kan anses ha ingripit jämförelsevis djupt i hemligheten i fråga om ett förtroligt meddelande. Som motvikt till den begränsade underrättelseskyldigheten enligt paragrafen, ska i lagen om övervakning av underrättelseverksamheten ( / ) föreskrivas om en allmän rätt att anföra klagomål hos underrättelseombudsmannen eller göra en begäran om undersökning. I Europadomstolens avgörandepraxis har en snävare underrättelseskyldighet ansetts godtagbar, om den part som upplever sig utan grund ha blivit föremål för en underrättelseinhämtningsåtgärd har en vidsträckt möjlighet att anföra klagomål eller annars föra sin sak för undersökning till en myndighet som står utanför underrättelseverksamheten.

Lagrad kommunikation ska kunna behandlas automatiskt och manuellt. Vid den fortsatta behandlingen av den information som samlats in på detta sätt ska man igen få reda ut meddelandets förmedlingsuppgifter, lokaliseringsuppgifter och meddelandets innehåll. I det moment det nu är fråga om ska det förutsättas att föremålet underrättas när den manuella fortsatta behandlingen av en uppgift har inriktats på innehållet i ett förtroligt meddelande. Det att det föreligger en underrättelseskyldighet förutsätter dessutom att den manuella behandlingen har inriktats på innehållet i ett förtroligt meddelande hos en person som befinner sig i Finland. I fråga om den manuella behandlingen av innehållet i ett förtroligt meddelande hos en person som befinner sig någon annanstans än i Finland ska det däremot inte finnas någon underrättelseskyldighet redan av den orsaken att detta ofta är omöjligt t.ex. för att man inte känner till föremålets riktiga identitet eller för att man inte känner till var föremålet, vars identitet i sig har fastställts, befinner sig eller med ett skäligt arbete kan reda ut det.

Underrättelseinhämtning som avser datatrafik hos någon annan än en statlig aktör, där innehållet i ett förtroligt meddelande reds ut, kan anses vara nära jämställt med teleavlyssning både i tekniskt hänseende och vad gäller hur djupt ingripandet i de grundläggande fri- och rättigheterna går. Därför föreslås det att om skyldigheten att underrätta föremålet om båda de nämnda metoderna ska föreskrivas på samma sätt.

Enligt momentet ska skyldighet att underrätta personen emellertid inte föreligga, om den information som inhämtats med underrättelseinhämtning som avser datatrafik har utplånats med stöd av 83 §. Det ska vara frågan om ett undantag från det som föreskrivs i första meningen. Således, om man vid behandlingen av kommunikation har rett ut innehållet i ett meddelande från en viss person som befinner sig i Finland, men man i samband med detta har upptäckt att informationen ska utplånas genast, och denna information som ska utplånas genast i enlighet med skyldigheten utan dröjsmål hade utplånats, föreligger ingen underrättelseskyldighet. Skyldigheten att underrätta föremålet om underrättelseinhämtning som avser datatrafik kan i dylika fall inte anses motiverad, eftersom underrättelsemyndigheterna efter utplåningen inte längre har information om den person som borde underrättas om saken.

Enligt 3 mom. i paragrafen ska personen i fråga underrättas om användningen av en metod för underrättelseinhämtning senast ett år från det att användningen upphörde. Om användningen av en metod de facto har avslutats medan tillståndet eller beslutet fortfarande är i kraft och något nytt tillstånd inte har sökts, ska tidsfristen på ett år räknas från den tidpunkt då informationsinhämtningen de facto avslutades. Om informationshämtningen avslutats då giltighetstiden för tillståndet eller beslutet gått ut, ska tidsfristen på ett år räknas från denna tidpunkt. I fråga om retroaktiv användning av en metod för underrättelseinhämtning ska tidsfristen räknas från den tidpunkt då tillståndet beviljades eller beslutet fattades, trots att information inte ännu fåtts.

Om det i fråga om samma person som är föremål för en metod för underrättelseinhämtning har fattats ett nytt beslut om användning av samma metod för underrättelseinhämtning, ska tidsfristen på ett år räknas från den tidpunkt då den sista informationsinhämtningen i ärendet de facto avslutades eller från utgången av tillståndets eller beslutets giltighetstid. Med tanke på informationsinhämtningens kontinuitet kan några dagars avbrott mellan beslutens giltighet godtas.

Enligt 4 mom. i paragrafen ska, om den som är föremål för en metod för underrättelseinhämtning inte är identifierad vid utgången av den tid eller det uppskov som avses i 1–3 mom., han eller hon utan ogrundat dröjsmål skriftligen meddelas om användningen av metoden för underrättelseinhämtning när identiteten har utretts. Om den person som är föremål för informationsinhämtningen har förblivit okänd, kan denne naturligtvis inte underrättas. Om man senare får reda på identiteten hos den som är föremål för en metod för underrättelseinhämtning, ska denne dock underrättas. Sådana situationer kan också utgöra undantag när det gäller de i paragrafen nämnda tidsfristerna, eftersom dessa i vissa fall inte kan iakttas. Om identiteten på den som är föremål för användningen av metoder för informationsinhämtning är känd men personen i fråga är försvunnen, förutsätts militärunderrättelsemyndigheterna inte vidta några omfattande åtgärder enbart för att underrätta denne.

Enligt 5 mom. ska den domstol som beviljat tillståndet samtidigt skriftligen informeras om underrättelsen. Följaktligen ska underrättandet av föremålet för en metod för underrättelseinhämtning som har förutsatt tillstånd också ges Helsingfors tingsrätt för kännedom.

Enligt 6 mom. ska domstolen på yrkande av Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman få besluta att underrättelsen enligt 1 eller 2 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, med avseende på landets försvar eller för att garantera den nationella säkerheten eller skydda liv eller hälsa. Domstolen ska få besluta att underrättelsen helt ska utebli, om det är nödvändigt för att trygga det militära försvaret eller den nationella säkerheten eller skydda liv eller hälsa.

Beslut om att underrättelsen ska skjutas upp eller helt utebli ska fattas av domstolen, även om det är fråga om en sådan metod för underrättelseinhämtning om vilken en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman har beslutat om. Enligt förslaget får underrättelsen skjutas upp med högst två år åt gången. Ett nytt uppskov ska beviljas endast i undantagsfall. Om förutsättningar finns ska det, i stället för upprepade uppskov med underrättelsen, ansökas om att någon underrättelse inte behöver göras, eftersom en underrättelse som görs t.ex. efter tio år inte har någon betydelse för den som varit föremål för informationsinhämtningen. Uppskov och förnyat uppskov ska sökas före utgången av tidsfristen.

Uppskov kan för det första beviljas för att trygga pågående användning av en metod för underrättelseinhämtning. Informationsinhämtningen ska kunna anknyta till vilken som helst pågående underrättelseinsats, också till en civil underrättelseinsats.

Uppskov ska också vara möjligt med tanke på landets försvar eller skyddandet av den nationella säkerheten. Detta innebär att för handen måste vara ett hot som riktar sig mot landets försvar, staten eller samhället. Till exempel våldsdåd som riktar sig mot enskilda personer kan emellertid ingå i landets försvar eller den nationella säkerheten, om de till sin omfattning eller betydelse är betydande med tanke på landets försvar eller den nationella säkerheten och således kan utgöra ett allvarligt hot mot dessa.

Dessutom ska ett uppskov kunna motiveras med skyddande av liv eller hälsa. Som förutsättning för uppskov anges att det ska vara motiverat. Tröskeln för ett uppskov kan sålunda inte anses vara särskilt hög.

Enligt en domstols beslut får underrättelsen helt utebli endast om det är nödvändigt för att trygga landets försvar eller den nationella säkerheten eller för att skydda liv eller hälsa. Tröskeln ska således vara hög.

Enligt 7 mom. behöver den som 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.

I fråga om platsspecifik underrättelseinhämtning ska den som har varit föremål för metoden för underrättelseinhämtning i fråga samt vid behov också platsens ägare eller innehavare underrättas om detta. I fråga om den kopiering och försändelsekopiering som avses i bestämmelsen ska föremålet för informationsinhämtningen underrättas om saken.

Vid militär underrättelseinhämtning ska information inte inhämtas för brottsbekämpning eller förundersökning. Ifall dylik information kommer till militärunderrättelsemyndigheternas kännedom, ska informationen kunna ges i enlighet med det förfarande om vilket föreskrivs i 76 och 77 §. Om förundersökning inleds utgående från information som getts i enlighet med vad som föreskrivs i 76 eller 77 §, ska vad som föreskrivs i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen iakttas.

Enligt momentet behöver någon underrättelse om användning av de i momentet nämnda metoderna för underrättelseinhämtning inte göras, om förundersökning inte ska inledas i det ärende som gäller metoderna i fråga.

I 8 mom. ska det föreskrivas att en statlig aktör inte behöver underrättas. När en metod för underrättelseinhämtning som riktar sig mot en statlig aktör och sker på finskt territorium används, anknyter till verksamheten nästan utan undantag utrikespolitiska och eventuellt också andra känsliga omständigheter, varvid det inte är motiverat att underrätta en person som varit föremål för en metod. Bestämmelsen hindrar dock inte att en underrättelse görs, vilket beskrivs av formuleringen ”behöver inte underrättas”.

I 9 mom. föreslås en hänvisning till domstolsförfarandet. Ifall domstolen inte beviljar uppskov eller godkänner att en underrättelse helt uteblir, ska den som framställt yrkandet kunna anföra klagomål över beslutet hos Helsingfors hovrätt på det sätt som föreskrivs i 113 §.

## 8 kap. Försvarsmaktens tjänstemäns och värnpliktigas deltagande i militär underrättelseinhämtning samt internationell verksamhet

**87 §.** *Försvarsmaktens tjänstemäns deltagande i militär underrättelseinhämtning.* I paragrafen ska det föreskrivas om att en annan tjänsteman vid Försvarsmakten än en tjänsteman vid en militärunderrättelsemyndighet kan användas vid militär underrättelseinhämtning. Vid försvarsmaktens truppförband finns det enheter där tjänstemännen har utbildats bl.a. i användningen av hemliga metoder för inhämtande av information inom Försvarsmaktens brottsbekämpning. Vidare har vissa enheter annan särskild kompetens till följd av sina uppgifter, vilken kunde utnyttjas vid utövandet av befogenheterna till militär underrättelseinhämtning. Eftersom likartade befogenheter till informationsinhämtning ska utövas vid den militära underrättelseinhämtningen, måste dessa tjänstemän kunna användas när situationen kräver det för att resurserna ska kunna användas på adekvat sätt.

Enligt paragrafen ska dessa tjänstemän när de använder metoder för underrättelseinhämtning alltid göra det under uppsikt och övervakning av den militärunderrättelsemyndighet, för vars underrättelseuppdrag de andra tjänstemän som avses i paragrafen ska användas.

**88 §.** *Befogenheter för en reservist som tjänstgör i enlighet med värnpliktslagen*. Också reservister som tjänstgör i enlighet med värnpliktslagen ska vid behov kunna användas vid underrättelseverksamheten. Den samhälleliga situationens utveckling i en sådan riktning att befogenheterna under undantagsförhållanden måste tas i bruk är en långvarig process under vilken militärunderrättelsemyndigheterna i en viss situation kan bli tvungna att inhämta extra mycket underrättelseinformation om hur situationen utvecklas. I sådan verksamhet som avses i paragrafen ska värnpliktiga som fullgör sin beväringstjänst inte få användas, vilket beror på att syftet med beväringstjänsten inte omfattar utförande av de uppgifter som avses i paragrafen. Utöver detta måste man observera att utbildningen av dem som fullgör beväringstjänst pågår, och att de inte ännu har förutsättningar att utföra de uppgifter som avses i paragrafen. Vid bedömningen av vad som är tillräcklig utbildning ska särskild uppmärksamhet ägnas kunnandet i datasäkerhet och behandling av personuppgifter. I de situationer som avses i paragrafen ska reservisterna enligt behov avgränsas till sådana uppgifter där personuppgifter behandlas i så liten utsträckning som möjligt.

I fråga om dem som fullgör beväringstjänst i enlighet med värnpliktslagen ska det beaktas att de används när beredskapen höjs. I dessa situationer ska dock hänsyn tas till beväringarnas kunskaps- och färdighetsmässiga förutsättningar att sköta olika uppgifter. Detta kan t.ex. innebära hur långt en beväring har hunnit i sin utbildning. En reservist som kallats för att utföra uppgifter inom den militära underrättelseinhämtningen ska få utöva de befogenheter som avses i denna lag endast under uppsikt och övervakning av en tjänsteman som är anställd inom den militära underrättelseinhämtningen. Därmed överförs inte någon betydande utövning av offentlig makt på någon annan än en tjänsteman i de situationer som avses i paragrafen.

För reservister som tjänstgör i enlighet med värnpliktslagen ska gälla samma sekretessplikt som för de tjänstemän under vilkas uppsikt och övervakning de utför sina uppgifter, såsom det föreskrivs nedan.

Enligt paragrafens 1 mom. ska en reservist som har fått tillräcklig utbildning få bistå militärunderrättelsemyndigheterna vid radiosignalspaning, underrättelseinhämtning som avser utländska datasystem, behandling av tekniska data och inriktning av underrättelseinhämtning som avser datatrafik.

När det bedöms om en reservist har tillräcklig utbildning, ska reservistens kunskaps- och färdighetsmässiga förutsättningar beaktas samt hur lång tid det har hunnit förflyta sedan reservisten fick sin utbildning.

Vid underrättelseinhämtning som avser datasystem ska det vara möjligt att använda en reservist t.ex. vid utvecklandet av datatekniska metoder som möjliggör skydd av ett datasystem och hävning av skyddet. Själva underrättelseinhämtningen som avser en främmande stats datatrafik ska dock en tjänsteman vid en militärunderrättelsemyndighet använda. Utövandet av befogenheten i fråga kan ha betydande konsekvenser, vilket gör att utövandet av den ska vara möjligt endast för en tjänsteman vid en militärunderrättelsemyndighet.

En reservist ska också kunna användas för att bistå vid inriktningen av underrättelseinhämtning som avser datatrafik. I de fall det är frågan om ska en reservist kunna utnyttja främst tekniska data om datatrafiken och statistiska analyser, som upprättats utifrån dem, och utgående från dessa analyser kan reservisten bistå de tjänstemän som särskilt utbildats i användningen av metoder för underrättelseinhämtning i att identifiera väsentliga delar av kommunikationsnät, där insamlandet och lagrandet av datatrafik är ändamålsenligast och kan genomföras med den bästa inriktningen. En reservist som bistår verksamheten, ska inte få behandla uppgifter som inhämtas vid underrättelseinhämtning som avser datatrafik, såsom innehållet i förtroliga meddelanden.

På motsvarande sätt som när det gäller att bistå vid inriktningen av underrättelseinhämtning som avser datatrafik, ska biståendet vid radiosignalspaning inriktas på det tekniska genomförandet av radiosignalspaning under uppsikt och övervakning av en tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning, såsom insamlande av radiosignaler, identifiering av väsentliga radiosignaler, inriktning av radiosignalspaningen samt hävning av kryptering.

I 2 mom. ska det föreskrivas om befogenheter för en reservist som skyndsamt har förordnats till en repetitionsövning, extra tjänstgöring eller tjänstgöring under mobilisering.

I situationer med ett skyndsamt förordnande till repetitionsövning är det fråga om ett förfarande enligt 32 § 4 mom. i värnpliktslagen. Republikens president kan på föredragning av kommendören för Försvarsmakten, när ett tvingande behov som uppstår i Finlands säkerhetspolitiska omgivning förutsätter det, förordna värnpliktiga som hör till reserven på repetitionsövning för att flexibelt höja den militära beredskapen. Ett behov som uppkommer i den säkerhetspolitiska omgivningen kan vara t.ex. en ovanlig militär övning som ordnas i Finlands närområde eller en annan situation som utvecklar sig hotfullt.

De metoder för underrättelseinhämtning som uttryckligen nämns i paragrafen, med undantag av teknisk avlyssning, är till sin art sådana att de värnpliktiga har kunnat få tillräcklig utbildning i och förtrogenhet med dem utifrån beväringstjänsten och repetitionsövningarna och dessa metoder ingriper inte i skyddet för hemligheten i fråga om ett förtroligt meddelande. I andra meningen i momentet ska det finnas ett särskilt omnämnande av att de metoder för underrättelseinhämtning som avses i momentet inte får användas för att reda ut innehållet i ett meddelande.

I paragrafens 3 mom. ska det föreskrivas om befogenheterna för en person som i enlighet med 47 § i lagen om försvarsmakten har tagit avsked från Försvarsmakten och deltar i en repetitionsövning. En person som blivit tvungen att ta avsked med stöd av paragrafen ovan kan ännu behövas i den militära underrättelseverksamheten och personen kan ha samlat på sig bety-

dande kunnande medan han eller hon var anställd vid en militärunderrättelsemyndighet. I vissa situationer kan detta kunnande ännu behöva användas också efter att personen har blivit tvungen att ta avsked från militärunderrättelsemyndigheten. Endast de personer kommer i fråga som med stöd av lagen måste ta avsked från militärunderrättelsemyndigheterna.

Enligt 4 mom. ska en reservist som avses i paragrafen få använda befogenheter endast under uppsikt och övervakning av en tjänsteman som är särskilt förtrogen med användning av metoder för underrättelseinhämtning.

**89 §.** *Deltagande i Försvarsmaktens internationella verksamhet.* I paragrafen ska det föreskrivas om användning i internationella uppdrag av för uppdraget förordnade och med användningen av metoder för underrättelseinhämtning särskilt förtrogna militärjurister och andra tjänstemän samt reservister. De situationer som avses i paragrafen ska inte vara underrättelseinsatser som militärunderrättelsemyndigheterna utför utanför Finlands gräns och om vilka föreskrivs i 62 §, utan de ska grunda sig på ett beslut av Finland antingen om att bistå en annan stat eller om att delta i en militär krishanteringsinsats i enlighet med lagen om militär krishantering. I internationell verksamhet som avses ovan är det typiskt att som en del av en nationell eller multinationell trupp finns underrättelseenheter eller underrättelseofficerare, som huvudsakligen agerar i enlighet med föreskrifter och anvisningar från den organisation som leder insatsen. Underrättelseenheterna och underrättelseofficerarna har till uppgift att producera information om omgivningen i de finska truppernas verksamhetsområde som stöd för det nationella beslutsfattandet och planeringen av truppernas egenskydd och verksamhet.

Enligt 1 mom. ska en person som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning, som har tagit avsked från en militärunderrättelsemyndighet i enlighet med 47 § i lagen om försvarsmakten och som har tagits i ett anställningsförhållande till Försvarsmakten kunna vara chef för en underrättelseenhet som är verksam vid givandet av internationellt bistånd eller i samband med en krishanteringsinsats. En person som är anställd vid en militärunderrättelsemyndighet kan enligt 47 § i lagen om försvarsmakten bli tvungen att ta avsked från en militär tjänst redan som 55-åring. Efter detta övergår personen till reserven. En reservist kan emellertid tas i ett anställningsförhållande i enlighet med lagen om militär krishantering eller i ett anställningsförhållande inom internationellt bistånd. Eftersom de personer som avses i paragrafen har det kunnande inom underrättelsesektorn som behövs, ska de kunna användas i internationell verksamhet som chef för en underrättelseenhet och denna chef ska kunna fatta beslut om användningen av de metoder för underrättelseinhämtning som avses i 4 kapitlet.

Enligt 2 mom. ska också andra reservister kunna användas i insatser som anknyter till givandet av internationellt bistånd eller i underrättelseverksamhet i samband med en militär krishanteringsinsats. I dessa uppdrag ska en person som står i ett anställningsförhållande till Försvarsmakten få utöva de befogenheter som avses i denna lag under uppsikt och övervakning av chefen för underrättelseenheten.

En reservist som avses i momentet ska ha fått tillräcklig utbildning. I fråga om vad som avses med detta hänvisas till vad som sägs i fråga om tillräcklig utbildning för reservister i detaljmotiveringen tidigare i detta kapitel.

Enligt 3 mom. ska Huvudstabens underrättelsechef besluta om deltagande i fråga om en i denna paragraf avsedd person som använder metoder för underrättelseinhämtning. Med beslutet ska avses deltagande i internationell verksamhet för vissa personer som använder metoder för underrättelseinhämtning, inte beslut att delta i givandet av internationellt bistånd eller i en

militär krishanteringsinsats eller mera vidsträckt beslut om de truppförband och personer som ska sändas ut på dessa insatser. Eftersom det alltid ska vara fråga om tjänstemän som är särskilt förtrogna med användningen av metoder för underrättelseinhämtning eller reservister som fått tillräcklig utbildning, ska Huvudstabens underrättelsechef ha ansvaret för att de tjänstemän eller reservister som deltar i internationell verksamhet är tillräckligt förtrogna med saken för att kunna vara verksamma i det uppdrag det nu är fråga om.

Enligt momentet ska Huvudstabens underrättelsechef också besluta om de personer som kan fatta beslut om att använda en metod för underrättelseinhämtning vid givandet av internationellt bistånd och i annan internationell verksamhet samt vid en militär krishanteringsinsats.

**90 §.** *Tjänsteansvar för den som tjänstgör i enlighet med värnpliktslagen.* På den som tjänstgör i enlighet med värnpliktslagen och utövar en sådan befogenhet som avses i 87 eller 88 § tillämpas bestämmelserna om straffrättsligt tjänsteansvar.

**91 §.** *Skadeståndsansvar för den som tjänstgör i enlighet med värnpliktslagen*. För en skada som orsakats i samband med en uppgift som avses i 88 § ska staten svara i enlighet med vad som föreskrivs i skadeståndslagen (412/1974).

Enligt 2 mom. ska på skadeståndsansvaret för den som utför en uppgift som avses i 88 § tillämpas bestämmelserna om en värnpliktigs skadeståndsansvar i 4 kap. i skadeståndslagen.

Enligt bestämmelserna i 3 kap. i skadeståndslagen är arbetsgivaren skyldig att ersätta en skada som arbetstagare förorsakar genom fel eller försummelse i arbetet (1 § 1 mom.). Om någon som på grund av ett förordnade av myndighet utför ett visst uppdrag som är fastställt genom lag utan att vara självständig företagare genom fel eller försummelse vållar skada då han fullgör uppdraget, är den för vars räkning uppdraget utförs skyldig att ersätta skadan (1 § 3 mom.). En beväring har i ett offentligrättsligt rättsförhållande ansetts vara en anställd, för vilken det offentliga samfundet kan få ett skadeståndsansvar.

Utifrån en föreskrift som meddelats med stöd av värnpliktslagen eller en annan motsvarande föreskrift har en person som är anställd hos staten enligt 4 kap. 2 § 2 mom. i skadeståndslagen samma ansvar som en tjänsteman eller arbetstagare. En militärperson ska ersätta en skada i den mån som bedöms vara skäligt med hänsyn till skadans storlek, handlingens beskaffenhet, skadevållarens ställning, den skadelidandes behov samt övriga omständigheter. En särskild ställning har enligt 3 mom. de militärpersoner som har orsakat en skada medan de ansvarade för säkerheten på ett militärt fartyg eller luftfartyg.

Det som sägs ovan betyder också en möjlighet till jämkning av skadestånd med beaktande av bl.a. skadans storlek, handlingens beskaffenhet och skadevållarens ställning. Om personen endast har gjort sig skyldig till lindrigt vållande, döms inte till skadestånd. När det är fråga om ett avsiktligt brott, är regeln att fullt skadestånd döms ut. Statens rätt till regression av skadevållaren har också den begränsats enligt 4 kap. 3 §.

För att statens husbondeansvar ska kunna utsträckas också till personer i sådana uppdrag som avses i 87 och 88 §, förutsätts att en bestämmelse om detta tas in i denna lag. Således behöver skadeståndslagen inte ändras.

9 kap. **Yppandeförbud, skyldigheter och rättigheter som gäller teleföretag och dataöverförare samt användning och erhållande av information**

**92 §.** *Yppandeförbud.* Enligt första meningen i 1 mom. får en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman förbjuda en utomstående att röja sådana omständigheter om användningen av en metod för underrättelseinhämtning som denne fått kännedom om, om det är motiverat för skyddandet av användningen av metoden för underrättelseinhämtning.

Grund för användningen av en metod för underrättelseinhämtning är alltid, att den verksamhet som är föremål för militär underrättelseinhämtning till sin art är militär eller att den utgör ett hot eller ett allvarligt hot mot den nationella säkerheten. När en metod för underrättelseinhämtning används är det möjligt att man råkar i en situation där utomstående bistånd behövs eller till och med är nödvändigt. Till exempel vid platsspecifik underrättelseinhämtning kan man behöva be det bolag som ansvarar för ett husbolags underhåll om tjänster. Således kan utomstående få uppgifter, som, om de röjs, kan äventyra åtminstone användningen av en metod för underrättelseinhämtning, men som samtidigt också utgör ett hot mot landets försvar eller den nationella säkerheten. Avsikten är att minska risken för att användningen av en metod för underrättelseinhämtning avslöjas samt att samtidigt skydda också taktiska och tekniska metoder som ska hemlighållas och i sista hand landets försvar och den nationella säkerheten.

Enligt andra meningen i 1 mom. 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 kan därmed inte meddelas vem som helst, t.ex. en boende i ett husbolag eller någon annan utomstående som råkar upptäcka att en anordning för teknisk observation har installerats.

I bestämmelsen ska med användning av en metod för underrättelseinhämtning avses användning av metoder för underrättelseinhämtning mera vidsträckt, vilket t.ex. ska inbegripa skyddande av användningen av de metoder för underrättelseinhämtning som ska användas vid militär och civil underrättelseinhämtning när militärunderrättelsemyndigheterna och skyddspolisen samarbetar. Det ska vara befogat att meddela ett yppandeförbud åtminstone om användningen av en metod för underrättelseinhämtning kan avslöjas om en utomstående inte meddelas ett förbud.

Enligt 2 mom. ska 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 hot om straff för överträdelse av förbudet. Momentet motsvarar 5 kap. 48 § 3 mom. i polislagen.

Militärunderrättelsemyndigheterna ska dessutom till beslutet foga tillräckliga anvisningar om hur den person som är föremål för ett yppandeförbud kan anmäla detta till underrättelseombudsmannen och begära att denne vidtar nödvändiga åtgärder samt information om hur den person soom har meddelats ett yppandeförbud kan anföra klagan över det till hovrätten. På detta sätt fullgör militärunderrättelsemyndigheterna också sin rådgivningsskyldighet, om vilken föreskrivs i 8 § 2 mom. i förvaltningslagen.

Rättsskyddet för en person som meddelats ett yppandeförbud garanteras också av den anmälan som militärunderrättelsemyndigheterna med stöd av 105 § ska göra till underrättelseombudsmannen om ett yppandeförbud.

I 3 mom. ska finnas bestämmelser om besvärsförbud i fråga om ett beslut som gäller yppandeförbud. Enligt bestämmelsen ska ett beslut om yppandeförbud inte få överklagas genom be-

svär. Den som har fått ett förbud får dock utan tidsbegränsning anföra klagan. Klagan ska behandlas skyndsamt.

Ett beslut om yppandeförbud ska alltid meddelas till underrättelseombudsmannen.

I ett beslut om yppandeförbud ska inbegripas ett tillkännagivande om med stöd av vilken bestämmelse det inte är möjligt att överklaga beslutet om yppandeförbud. Yppandeförbudet ska inte förhindra den som meddelats förbudet att meddela detta till underrättelseombudsmannen.

Besvärsförbudet gällande ett beslut om yppandeförbud behandlas nedan under rubriken förhållande till grundlagen och lagstiftningsordning.

Enligt 4 mom. 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. Bestämmelsen i momentet motsvarar 5 kap. 48 § 3 mom. i polislagen.

I 5 mom. ska det föreskrivas om rätt för den som har meddelats ett yppandeförbud att trots 4 mom. meddela underrättelseombudsmannen om yppandeförbudet. Detta är motiverat med tanke på rättsskyddet för den som meddelats ett yppandeförbud. På detta sätt kan var och en som meddelats ett yppandeförbud trots förbudet meddela underrättelseombudsmannen sin syn på saken.

**93 §.** *Teleföretags biståndsskyldighet.* Enligt 1 mom. ska ett teleföretag utan ogrundat dröjsmål göra de kopplingar i ett telenät som behövs för teleavlyssning och teleövervakning samt tillhandahålla militärunderrättelsemyndigheterna de uppgifter och redskap samt den personal som behövs för att teleavlyssning ska kunna utföras. Detsamma gäller också de situationer där militärunderrättelsemyndigheterna genomför teleavlyssning eller teleövervakning med hjälp av en teknisk anordning. Teleföretaget ska dessutom ge militärunderrättelsemyndigheten sådana uppgifter som företaget innehar och som behövs för teleavlyssning eller teleövervakning. Teleavlyssning och teleövervakning ska också kunna genomföras med militärunderrättelsemyndigheternas egna anordningar.

Enligt gällande polislag har polisen rätt att använda teleavlyssning och teleövervakning. Vid militär underrättelseinhämtning ska användas samma tekniska lösning och system som polisen använder. Detta innebär att ett andra motsvarande system som möjliggör teleavlyssning och teleövervakning inte behöver byggas endast för militärunderrättelsemyndigheternas befogenheter.

Enligt paragrafen ska ett teleföretag tillhandahålla militärunderrättelsemyndigheterna de uppgifter och redskap samt den personal som behövs för att teleavlyssning och teleövervakning ska kunna utföras. Paragrafen motsvarar i sak 5 kap. 61 § 1 mom. i polislagen.

**94** *§. Dataöverförarens skyldighet att medverka till genomförandet och upprätthållandet av den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter*. I paragrafen ska det föreskrivas om dataöverförarens biståndsskyldighet. Biståndsskyldigheten ska bestå av genomförande av en accesspunkt samt givande till Försvarsmaktens underrättelsetjänst av sådana uppgifter som dataöverföraren innehar och som har betydelse när det gäller att identifiera en viss del av kommunikationsnätet som överskrider Finlands gräns.

I 1 mom. ska det föreskrivas om en dataöverförares skyldighet att medverka. Enligt momentet ska dataöverföraren vara skyldig att i samarbete med Försvarsmaktens underrättelsetjänst

medverka till att de accesspunkter som förutsätts för underrättelseinhämtning som avser datatrafik kan genomföras för Försvarsmaktens underrättelsetjänsts räkning. Momentet ska vidare innehåll en skyldighet för dataöverföraren att medverka till att accesspunkten upprätthålls.

Enligt momentet ska dataöverföraren ha rätt att delta i de åtgärder som förutsätts för att accesspunkterna ska kunna genomföras. Syftet med accesspunkten är att möjliggöra att Försvarsmaktens underrättelsetjänst får tillträde till den datakommunikationsförbindelse som överskrider Finlands gräns och som stämmer överens med domstolens tillstånd och till den datatrafik som rör sig i denna förbindelse.

Med medverkan ska avses samarbete vid genomförandet av accesspunkten. I praktiken ska detta avse Försvarsmaktens underrättelsetjänsts och dataöverförarens plan för hur det tekniskt är mest ändamålsenligt att genomföra accesspunkten. Vidare ska dataöverföraren ha rätt att delta i de åtgärder som förutsätts för att en accesspunkt ska kunna anläggas. Anslutningen ska administreras av den som utför kopplingen.

Ändamålsenligast ska det vara att genomföra en accesspunkt så nära som möjligt till den kommunikationsnätsdel som överskrider Finlands gräns och som dataöverföraren äger eller administrerar. I praktiken är detta inte alltid ändamålsenligt, vilket gör att med medverkan av dataöverföraren ska en accesspunkt också kunna genomföras på ett annat ändamålsenligt ställe i det kommunikationsnät som ägs eller administreras av dataöverföraren.

Den medverkan och det samarbete som avses i momentet ska vara utgångspunkt för genomförandet av en accesspunkt och Försvarsmaktens underrättelsetjänst ska i första hand identifiera dataöverföraren och stå i kontakt med den i fråga om genomförandet av accesspunkten.

Med formuleringen upprätthålla i momentet ska avses dataöverförarens skyldighet att meddela sina planer på att göra ändringar i kommunikationsnätet, vilka kan ha omedelbar betydelse för accesspunktens funktion. Ändringar i kommunikationsnätet kan ske i och med att tekniken utvecklas, t.ex. nya tekniska lösningar installeras, eller annars på ett sådant sätt att väsentliga ändringar sker i nätets topologi. Upprätthållandet av accesspunkten ålägger inte dataöverföraren att aktivt utföra tekniska åtgärder i accesspunkten, utan det ska vara fråga om att hålla Försvarsmaktens underrättelsetjänst uppdaterad om de ändringar som planeras i nätet. Upprätthållandet av en accesspunkt förutsätter regelbundet samarbete mellan Försvarsmaktens underrättelsetjänst och dataöverföraren, t.ex. i form av möten fyra gången per år.

I de situationer om vilka föreskrivs i 2 mom. är det fråga om situationer där en accesspunkt inte kan genomföras med medverkan och deltagande av dataöverföraren. Det är fråga om ett undantag från bestämmelsen i 1 mom. I praktiken blir en sådan situation aktuell när dataöverföraren, trots Försvarsmaktens underrättelsetjänsts försök, inte aktivt vidtar åtgärder för att genomföra en accesspunkt.

Vidare ska bestämmelsen omfatta sådana situationer där dataöverföraren inte går att nå trots aktiva försök av Försvarsmaktens underrättelsetjänst.

**95 §.** *Dataöverförarens skyldighet att lämna uppgifter.* I paragrafen ska det föreskrivas att dataöverföraren till Försvarsmaktens underrättelsetjänst på dess specificerade begäran ska lämna de uppgifter som dataöverföraren förfogar över och som behövs för att identifiera den del av kommunikationsnätet som behövs för tillståndsyrkandet och tillståndsbeslutet i fråga om användningen av underrättelseinhämtning som avser datatrafik. Skyldigheten sammanhänger med 64 § 3 mom. 2 punkten, 66 § 3 mom. 3 punkten samt 68 § 3 mom. 5 punkten, vilka gäller

domstolens tillstånd till underrättelseinhämtning som avser datatrafik och enligt vilka Försvarsmaktens underrättelsetjänst i sitt tillståndsyrkande till domstolen ska specificera den del av kommunikationsnätet, där datatrafiken ska jämföras med automatiska sökbegrepp inom den underrättelseinhämtning som avser datatrafik. För att kommunikationsnätsdelen ska kunna specificeras för tillståndsyrkandet är det nödvändigt att Försvarsmaktens underrättelsetjänst får uppgifter som främjar specificerandet av de parter som innehar sådana uppgifter t.ex. av skäl som anknyter till parternas affärsverksamhet.

De uppgifter som dataöverföraren ska ge med stöd av den skyldighet som avses i paragrafen ska inte anknyta till utformandet av sökbegrepp med anledning av de bestämmelser som det hänvisas till ovan och inte heller till inhämtandet av förmedlingsuppgifter som anknyter till enskilda personer, utan det ska uttryckligen vara fråga om att identifiera en viss del av kommunikationsnätet.

Genom att det föreskrivs om skyldigheten att ge uppgifter kan det förhindras att en sökbaserad jämförelse skulle inriktas på datatrafiken i större utsträckning än vad som är nödvändigt för syftet med den militära underrättelseinhämtningen. Om uppgifter som dataöverföraren innehar visar att datatrafik som gäller den verksamhet som är föremål för informationsinhämtning inte kan röra sig i en viss del av kommunikationsnätet, t.ex. därför att den delen är reserverad för en kundorganisation som är oviktig med tanke på den verksamhet som är föremål för underrättelseinhämtning som avser datatrafik, kan den delen av kommunikationsnätet inte inbegripas i ett tillståndsyrkande som gäller underrättelseinhämtning som avser datatrafik.

De uppgifter som är nödvändiga för att inrikta underrättelseinhämtning som avser datatrafik och som avses i paragrafen ska gälla nätets tekniska realiseringssätt och topologi t.ex. i fråga om ett visst geografiskt område. Enligt paragrafen ska dataöverföraren inte kunna åläggas att överlåta uppgifter som anknyter till en enskild fysisk eller juridisk person som är kund.

Utgående från de uppgifter som avses i paragrafen ska Försvarsmaktens underrättelsetjänst kunna bedöma t.ex. sannolikheten för att datatrafik dirigeras genom den del av kommunikationsnätet som dataöverföraren äger eller annars innehar. Paragrafen ska inte annars heller ge Försvarsmaktens underrättelsetjänst rätt att inhämta eller få uppgifter som gäller en enskild kommunikationshändelses förmedlingsuppgifter eller innehållet i ett meddelande.

Bestämmelsen i paragrafen ska förplikta dataöverföraren att ge Försvarsmaktens underrättelsetjänst sådana uppgifter som är nödvändiga för att den underrättelseinhämtning som avser datatrafik ska kunna inriktas. Det krav som gäller att uppgifterna ska vara nödvändiga ska inbegripa att dataöverföraren till Försvarsmaktens underrättelsetjänst ska lämna alla sådana uppgifter som kan ha betydelse med tanke på att den underrättelseinhämtning som avser datatrafik ska kunna inriktas så exakt som möjligt. Å andra sidan följer det av kravet på att uppgifterna ska vara nödvändiga att dataöverföraren inte ska vara förpliktad att lämna Försvarsmaktens underrättelsetjänst sådana uppgifter som inte har betydelse med tanke på inriktningen. Vidare ska dataöverföraren med stöd av bestämmelsen inte vara förpliktad att på krav av Försvarsmaktens underrättelsetjänst utarbeta rapporter som är av betydelse med tanke på inriktningen eller inhämta annan information som dataöverföraren inte redan innehar eller som dataöverföraren inte annars producerar t.ex. i anknytning till sin affärsverksamhet.

Dataöverförarens skyldighet att lämna uppgifter ska endast gälla sådana uppgifter som den redan innehar. Den skyldighet att lämna uppgifter som föreslås ska således inte förplikta dataö-

verförarna att inhämta eller samla in sådana nya uppgifter för Försvarsmaktens underrättelsetjänst räkning som i sig kan behövas när det gäller att inrikta underrättelseinhämtning som avser datatrafik.

Skyldigheten att bistå ska förutsätta en specificerad begäran av en till uppdraget av Försvarsmaktens underrättelsetjänst förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. I begäran ska Försvarsmaktens underrättelsetjänst ange de uppgifter utgående från vilka dataöverföraren kan bedöma vilka av de uppgifter den innehar som kunde behövas för att definiera en viss del av det kommunikationsnät som överskrider Finlands gräns. Begäran ska inte kunna gälla en obestämd och obegränsad datamängd, som dataöverföraren ska ge uppgifter om med stöd av biståndsskyldigheten.

Dataöverföraren ska i fråga om begäran som avses i paragrafen ha möjlighet att framställa en begäran om undersökning eller anföra klagomål hos underrättelseombudsmannen med stöd av lagen om övervakning av underrättelseverksamheten, om dataöverföraren anser att militärunderrättelsemyndigheten har förfarit osakligt. Detta påverkar emellertid inte dataöverförarens skyldighet att till militärunderrättelsemyndigheterna överlåta de uppgifter som avses i paragrafen och dataöverföraren ska följaktligen överlåta uppgifterna.

**96 §.** *Ersättningar till teleföretag.* I 1 mom. föreskrivs det att ett teleföretag har rätt att få ersättning av statens medel för direkta kostnader som orsakats av att företaget i enlighet med detta kapitel har bistått myndigheterna och lämnat uppgifter, så som föreskrivs i 299 § i lagen om tjänster inom elektronisk kommunikation. Försvarsmakten ska besluta om ersättning av kostnaderna.

**97 §.** *Ersättningar till dataöverförare.* I paragrafen ska det föreskrivas om ersättning för de kostnader som en dataöverförare har orsakats av att lämna uppgifter och om vem som fattar beslut om ersättning.

Enligt momentet ska en dataöverförare ha rätt att få ersättning av statens medel för direkta kostnader som orsakats av sådant bistående som avses i 94 och 95 §. De direkta kostnader som avses i momentet ska huvudsakligen vara arbetskraftskostnader. Direkta kostnader ska också kunna vara kostnader för användning av teknisk utrustning och andra hjälpmedel som utnyttjats när uppgifterna sammanställdes. Försvarsmaktens underrättelsetjänst ska besluta om utbetalning av ersättningen. Följaktligen avgör Försvarsmaktens underrättelsetjänst vilka kostnader som är direkta och ska ersättas. Försvarsmaktens underrättelsetjänst ska också fastställa storleken på ersättningen.

Paragrafen gäller också de kostnader som orsakas av det tekniska genomförandet av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning. Också i dessa fall ska Försvarsmaktens underrättelsetjänst fastslå vilka kostnader som ska ersättas.

**98 §.** *Sökande av ändring i ett ersättningsbeslut.* I 1 mom. ska det föreskrivas om hur man begär omprövning av ett beslut om ersättning till ett teleföretag eller en dataöverförare. I ett beslut som en militärunderrättelsemyndighet har fattat kan omprövning begäras hos den som fattat beslutet.

Enligt 2 mom. får ett beslut som meddelats med anledning av en begäran om omprövning överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996).

Enligt 3 mom. får besvär anföras över förvaltningsdomstolens beslut hos högsta förvaltningsdomstolen, om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Enligt 4 mom. ska Kommunikationsverket ges tillfälle att bli hörd vid behandlingen i förvaltningsdomstolen.

**99 §.** *Avgifter för kopplingen.* Enligt paragrafen ska den som utför en koppling få ta ut avgifter av Försvarsmaktens underrättelsetjänst för kopplingen. Avgifterna ska dock inte få överstiga beloppet av de totala kostnader som utförandet av kopplingen medför för den som utför kopplingen (självkostnadsvärde). Som utgångspunkt vid beräkningen av självkostnadsvärdet kan t.ex. användas de beräkningsgrunder som används för självkostnadsvärdet enligt 6 § 1 mom. i lagen om grunderna för avgifter till staten (150/1992).

Det är ändamålsenligt att betalningstransaktionerna anvisas till Försvarsmaktens underrättelsetjänst, som är teknisk genomförare av underrättelseinhämtning som avser datatrafik också för skyddspolisens räkning. Det tillstånd som skyddspolisen har fått av domstolen ska den lämna till Försvarsmaktens underrättelsetjänst, som utför det tekniska inhämtandet av uppgifter vid underrättelseinhämtning som avser datatrafik och till skyddspolisen i obehandlad form levererar det material underrättelsetjänsten har samlat in. Som en del av processen ska Försvarsmaktens underrättelsetjänst meddela den som utför kopplingen de delar av kommunikationsnätet som överskrider Finlands gräns, ur vilka datatrafik ska inhämtas.

**100 §.** *Användning av uppgifter som lagras av teleföretag.* I paragrafen ska det föreskrivas om teleföretagens skyldighet att lagra uppgifter som avses i 157 § 1 mom. i lagen om tjänster inom elektronisk kommunikation också för skötsel av uppgifter inom den militära underrättelseinhämtningen.

I 157 § 1 mom. i lagen om tjänster inom elektronisk kommunikation föreskrivs att uppgifter som avses i paragrafens 2 och 3 mom. får användas endast för att utreda och åtalspröva brott som avses i 10 kap. 6 § 2 mom. i tvångsmedelslagen. I den sist nämnda bestämmelsen finns en förteckning över brott som berättigar till teleövervakning.

Enligt den föreslagna paragrafen ska motsvarande uppgifter kunna användas också för att få information om militär verksamhet och verksamhet som allvarligt hotar den nationella säkerheten, vilka i sin tur definieras i 4 § i denna proposition. Därmed ska det inte vara fråga om att lagra nya uppgifter, utan om att utnyttja redan existerande uppgifter förutom för att reda ut och åtalspröva brott också för att sköta uppgifter inom militär underrättelseinhämtning. Mängden uppgifter som lagras kommer inte att öka.

**101 §.** *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 ska militärunderrättelsemyndigheterna enligt 1 mom. på begäran av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman ha rätt att av privata sammanslutningar få sådana uppgifter som i ett enskilt fall kan antas vara behövliga vid utredningen av sådan verksamhet som avses i 4 § och som kan anses vara av betydelse för att 1) identifiera en fysisk eller juridisk person som är föremål för militär underrättelseinhämtning, 2) inrikta användningen av en metod för underrättelseinhämtning på en viss person eller 3) klarlägga ekonomisk verksamhet som bedrivs av en fysisk eller juridisk person.

Momentet motsvarar till sitt syfte i mycket stor utsträckning 4 kap. 3 § 1 mom. i polislagen. I detta sammanhang ska föremål för begäran om information dock inte vara att förhindra eller reda ut ett brott, utan begäran om information ska vara bunden till de föremål för militär underrättelseinhämtning som avses i 4 §. Av denna anledning ska i paragrafen nämnas att de uppgifter som är föremål för begäran om information kan antas behövas för att reda ut verksamhet enligt 4 §.

Med formuleringen att reda ut verksamhet ska inte avses att reda ut ett brott i den betydelse som är förenlig med förundersökningslagen, utan det ska vara fråga om att reda ut en specificerad verksamhet som är föremål för militär underrättelseinhämtning. Med att reda ut ska därmed avses att sammanställa information genom att samla in uppgifter från olika källor och den begäran om information som avses i paragrafen ska vara en metod att samla in betydelsefulla uppgifter om föremålen för militär underrättelseinhämtning.

Momentet ska innehålla förutsättningar som kan jämställas med en förväntning om att verksamheten ger resultat. En för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman ska beakta förutsättningarna vid prövningen av begäran om information. Även om den som framför en begäran om information inte har någon skyldighet att motivera sig för den som överlåter informationen, ska han eller hon grunda sin prövning gällande begäran om information på objektiva omständigheter och registrera dessa för att det i efterhand med laglighetsövervakningens medel ska vara möjligt att verifiera att begäran om information är korrekt.

Syftet med bestämmelsen ska vara att göra det möjligt för en enskild part att överlåta en uppgift utan att göra sig skyldig till en straffbar gärning. Den som överlåter en uppgift som omfattas av företags-, bank- eller försäkringshemligheten ska vid överlåtelsen av uppgiften till militärunderrättelsemyndigheterna kunna vara övertygad om att han eller hon handlar på ett tillåtet sätt.

Bestämmelser om bankhemligheten finns i 15 kap. 14 § i kreditinstitutslagen (610/2014) och om försäkringshemligheten i 30 kap. 1 § i försäkringsbolagslagen (521/2008). I 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 emellertid att den bestämmelse det nu är fråga om ska ge rätt att till militärunderrättelsemyndigheten överlåta en uppgift som omfattas av den ovan angivna tystnadsplikten.

Företagen har många uppgifter som omfattas av företagshemligheten och som är av betydelse för deras egen näringsverksamhet, såsom produktutvecklingsuppgifter. Utgående från paragrafen ska ett företag inte vara skyldigt att till militärunderrättelsemyndigheterna överlåta uppgifter som hör till företagshemlighetens kärna, utan i princip ska det vid en begäran om information vara fråga om uppgifter som specificerar parter som står i en kund- eller arbetstagarrelation eller i en annan ekonomisk relation.

Huruvida det i en begäran om information är fråga om ett enskilt fall ska bedömas med tanke på föremålet för den militära underrättelseinhämtning som informationsinhämtningen gäller. Således ska ett enskilt fall inte begränsa antalet begäranden om information om verksamhet som är föremål för samma militära underrättelseinhämtning. Ett enskilt fall ska vid behov kunna avse flera begäranden om information som gäller verksamheten i fråga.

De uppgifter som är föremål för en begäran ska enligt 1 punkten med fog kunna antas vara av betydelse vid identifieringen av en fysisk eller juridisk person som är föremål för militär underrättelseinhämtning. Med detta ska avses att det kan antas att en person som är föremål för militär underrättelseinhämtning med tillgängliga uppgifter kan identifieras eller dennes verksamhet annars redas ut t.ex. utifrån ett hotells inkvarteringsförteckning eller passagerarförteckningen i ett fartyg. Enligt 2 punkten ska som grund för en begäran kunna anföras att användningen av en metod för underrättelseinhämtning ska kunna inriktas på en viss person. Detta ska innebära t.ex. att en begäran kan riktas till en minutförsäljningsaffär och gälla inköp av en pre paid -anslutning och köparen av den. Paragrafens 2 punkt ska gälla bl.a. bankförfrågningar och andra begäranden om information hos kreditinstitut eller penningförmedlingsaktörer.

Enligt 2 mom. ska militärunderrättelsemyndigheterna i ett enskilt fall på begäran ha rätt att av teleföretag och av sammanslutningsabonnenter få kontaktuppgifter för teleadresser som inte är upptagna i en offentlig katalog eller information som identifierar en teleadress eller teleterminalutrustning, om informationen behövs för att militärunderrättelsemyndigheterna ska kunna utföra ett underrättelseuppdrag. Militärunderrättelsemyndigheterna ska ha motsvarande rätt att få information om utdelningsadresser av en sammanslutning som bedriver postverksamhet.

Bestämmelsen ska i sak motsvara 4 kap. 3 § i polislagen. Det ska vara fråga om en sådan sedvanlig åtgärd med anknytning till underrättelseverksamheten som inte ska förutsätta begäran av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

## 10 kap. Övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen

**102 §.** *Intern övervakning*. Chefen för Huvudstaben ska övervaka den militära underrättelseverksamheten. Utöver detta svarar Försvarsmaktens assessor för den interna laglighetsövervakningen på den militära underrättelseinhämtningens verksamhetsområde. Den interna övervakningen av underrättelseverksamheten ska vara den främsta övervakningen och den ska kompletteras med extern laglighetsövervakning, om vilken ska föreskrivas i en särskild lag.

Det att ansvaret för den allmänna övervakningen av militär underrättelseverksamhet läggs på chefen för Huvudstaben och ansvaret för den interna laglighetsövervakningen läggs Försvarsmaktens assessor åsidosätter emellertid inte annan chefsövervakning. Med detta ska avses chefsövervakning som är en del av de normala arbetsledningsuppgifterna. Denna form av övervakning betonas, eftersom den försiggår varje dag och nära den verksamhet som ska övervakas.

Paragrafen ska komplettera den laglighetsövervakning som Försvarsmaktens assessor har anförtrotts enligt 5 § 1 mom. i statsrådets förordning om försvarsmakten. Också juridisk utbildning för personalen utgör en viktig del av den förebyggande interna laglighetsövervakningen.

**103 §.** *Övervakning som försvarsministeriet utför*. Enligt 68 § 1 mom. i grundlagen svarar varje ministerium inom sitt ansvarsområde för att förvaltningen fungerar som sig bör. Bestämmelser om ministeriernas ansvarsområden finns i reglementet för statsrådet. Enligt det hör till försvarsministeriets ansvarsområde försvarspolitik, militärt försvar, samordning av totalförsvaret samt militär krishantering och fredsbevarande verksamhet. Vidare finns bestämmelser om den övervakning som försvarsministeriet utför i lagen om militär disciplin och brottsbekämpning inom försvarsmakten.

Bestämmelser om försvarsministeriets övervakning av Försvarsmaktens militära underrättelseinhämtning ska finnas direkt i lag. För närvarande grundar sig övervakningen på de bestämmelser som beskrivs ovan. Enligt paragrafens 1 mom. ska försvarsministeriet i praktiken ha rätt att granska de beslut som fattats, upptagningar och handlingar som upprättats samt annat material som uppkommit inom den militära underrättelseinhämtningen.

I 2 mom. ska det föreskrivas om försvarsministeriets rätt att få uppgifter om samhälleligt, ekonomiskt eller till sin allvarlighetsgrad betydande omständigheter som anknyter till den militära underrättelseinhämtningen. I underrättelseverksamheten kan det uppkomma situationer som är känsliga framför allt utrikes- och säkerhetspolitiskt. Av detta skäl måste försvarsministeriet i god tid känna till de situationer som nämns i momentet. På så sätt kan försvarsministeriet och därigenom statsrådet på förhand förbereda sig på en situation på behövligt sätt.

**104 §.** *Extern övervakning av den militära underrättelseinhämtningen.* Försvarsministeriet ska årligen till riksdagens justitieombudsman och till underrättelseombudsmannen lämna en berättelse om hur metoderna för underrättelseinhämtning har använts och användningen övervakats.

**105 §.** *Anmälningar till underrättelseombudsmannen.* Enligt 1 mom. ska militärunderrättelsemyndigheterna informera underrättelseombudsmannen om de beslut och tillstånd som domstolen har beviljat med stöd av denna lag så snart som möjligt efter domstolens beslut.

Till följd av underrättelseverksamhetens art samt domstolens uppgift är det ändamålsenligt att militärunderrättelsemyndigheterna till underrättelseombudsmannen anmäler de tillstånd som domstolen har beviljat. Anmälningsskyldigheten ska också omfatta negativa beslut som domstolen har fattat på beslut i en brådskande situation samt de tillstånd och negativa beslut som domstolen har fattat och som avses i 40 § 2 mom. I praktiken blir informeringsskyldigheten uppfylld genom att en kopia av domstolens beslut lämnas till underrättelseombudsmannen. I samband med detta ska också en tillståndsansökan i saken kunna lämnas in till underrättelseombudsmannen.

En anmälan ska också utgöra en betydande del av den externa övervakningen av användningen av metoder för underrättelseinhämtning. Underrättelseombudsmannen ska ha aktuell information om vilka typer av befogenheter militärunderrättelsemyndigheterna ska utöva vid den militära underrättelseinhämtningen. Underrättelseombudsmannen ska övervaka bl.a. att militärunderrättelsemyndigheterna är verksamma inom de gränser som förutsätts i det tillståndsbeslut som domstolen har beviljat.

I paragrafens 2 mom. ska det föreskrivas om andra anmälningar som ska göras till underrättelseombudsmannen än dem som avses i 1 mom. Militärunderrättelsemyndigheterna ska utan oskäligt dröjsmål informera underrättelseombudsmannen om ett beslut som gäller 1) skyddandet av militär underrättelseinhämtning, 2) yppandeförbud, eller 3) uppskjutande av en anmälan som avses i 76 § 1 mom.

Viktigare än det anmälningsförfarande om vilket föreskrivs i 1 mom. är att underrättelseombudsmannen får information om annat än de tillstånd som domstolen beviljat. Möjliggörandet av en oberoende juridisk övervakning i dylika ärenden är de facto viktigt, eftersom de beslut som underrättelsemyndigheterna själva har fattat inte har genomgått en extern objektiv bedömning innan en metod för underrättelseinhämtning tagits i användning, tvärtemot vad som är fallet när domstolen beviljar tillstånd.

Enligt 3 mom. ska det vid anmälan av 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 de beslut som ska fattas om dem innehåller uppgifter som till sin art är mycket känsliga och sekretessbelagda. I samband med att de anmälningar som avses i paragrafen görs ska särskild uppmärksamhet ägnas att sekretessen förverkligas och datasäkerheten säkerställs. Anmälan till underrättelseombudsmannen ska göras på ett sådant sätt att detta inte medför en risk för att sekretessbelagd information avslöjas. Uppgifter som är föremål för en anmälan bör hanteras endast i sådana lokaler som har konstaterats till sin lokal- och konstruktionssäkerhet vara sådana att det är tryggt att hantera uppgifter i dem utan risk för att uppgifterna avslöjas.

Om anmälningsplikten genomförs med hjälp av automatisk databehandling, bör dataöverföringsförbindelsen vara sådan att den inte i sig orsakar risk för att sekretessbelagda uppgifter avslöjas. Åtminstone i fråga om de andra anmälningarna än de som avses i 1 mom. är det motiverat att man i underrättelsemyndigheternas lokaler bekantar sig med de beslut som ligger till grund för anmälan. Anmälan om ett beslut ska kunna göras genom förmedling av en sådan kommunikationsanordning som till sina tekniska egenskaper möjliggör att uppgifterna endast finns tillgängliga för underrättelseombudsmannen.

Anmälningsförfarandet ska inte utformas så att det i sig orsakar kostnader som är klart oproportionerliga i förhållande till realiserandet av syftet med den anmälan som ska göras till underrättelseombudsmannen.

11 kap. **Särskilda bestämmelser**

**106 §.** *Beräkning av tidsfrister*. Enligt 1 mom. ska vid beräkning av tidsfrister enligt denna lag inte tillämpas lagen om beräknande av laga tid **(**150/1930**)**. I 2 mom. föreskrivs det att 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. Den sista meningen avser t.ex. att om giltighetstiden för ett en månads tillstånd börjar den 31 mars, upphör tillståndets giltighet den 30 april.

**107 §.** *Granskning av upptagningar och handlingar.* Enligt bestämmelsen ska den tjänsteman som leder användningen av en metod för underrättelseinhämtning eller en av denne förordnad tjänsteman utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av metoder för underrättelseinhämtning enligt 4 kap. Den tjänsteman som ska utföra granskningen ska kunna fastslås t.ex. i det beslut som gäller användningen av en metod för underrättelseinhämtning.

Den tjänsteman som leder användningen av en metod för underrättelseinhämtning och framför allt den tjänsteman som använder metoden för underrättelseinhämtning har en central ställning när åtgärder vidtas och är skyldiga att övervaka att de vidtas på lagenligt sätt. Med stöd av bestämmelsen ska de upptagningar och handlingar som uppkommit vid användningen av metoder för underrättelseinhämtning granskas, och bl.a. sådant material som omfattas av förbud mot underrättelseinhämtning samt annat material som militärunderrättelsemyndigheterna inte får inhämta genom användning av en metod för underrättelseinhämtning ska utplånas ur upptagningarna och handlingarna. Granskningen behöver göras utan dröjsmål bl.a. för att material som omfattas av förbud mot underrättelseinhämtning ska kunna konstateras och förstöras.

Skyldigheten att granska upptagningar och handlingar ska inta en särskilt betydande roll vid övervakningen av att underrättelseverksamheten är lagenlig. Granskningen av upptagningar och handlingar har en väsentlig betydelse för att den tjänsteman som ansvarar för verksamheten de facto i realtid ska kunna övervaka att metoderna för underrättelseinhämtning används lagenligt.

Ifall uppdraget att granska upptagningar och handlingar har getts till en annan tjänsteman än den som leder användningen av en metod för underrättelseinhämtning eller den som använder metoden för underrättelseinhämtning, ska det sörjas för att den tjänsteman som genomför granskningen har tillräckliga kunskaper, färdigheter och erfarenhet för att fullgöra uppdraget.

Vid granskning av upptagningar och handlingar kan tekniska anordningar, metoder eller programvaror utnyttjas så att granskningen med hjälp av dem kommer att omfatta endast sådana delar av upptagningar som innehåller t.ex. kommunikation. Tomma delar kan på så sätt raderas eller förbigås.

Med paragrafens hänvisning ”utan ogrundat dröjsmål” ska avses att upptagningarna och handlingarna ska granskas så snart som möjligt. Ett grundat dröjsmål kunde bero t.ex. på att granskningen inte lyckas utan tolk och att det kan vara svårt att skaffa en sådan, eller också kan det hända att omvandling av upptagningarna till förståelig form kan förutsätta dekryptering.

Skyldigheten att granska upptagningar och handlingar garanterar på ett sätt som är viktigt med tanke på förutsebarheten och proportionaliteten i metoderna för informationsinhämtning att militärunderrättelsemyndigheterna inte på ett förbjudet sätt använder överskottsinformation, som inte anknyter till ett underrättelseuppdrag, till föremålet för underrättelseinhämtning eller som gäller utomstående. Å andra sidan möjliggör granskningen av upptagningar också att förutsättningarna för att fortgå med att använda en metod för underrättelseinhämtning kan redas ut och förhindrar militärunderrättelsemyndigheterna att upprätta otillåtna personregister.

**108 §.** *Undersökning av upptagningar.* Enligt 1 mom. ska de upptagningar som uppkommit vid användningen av en metod för underrättelseinhämtning få undersökas endast av domstolen, Huvudstabens underrättelsechef, en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman eller någon annan tjänsteman vid en militärunderrättelsemyndighet som förordnats till ett underrättelseuppdrag, såsom en analytiker. Med undersökning av upptagningar avses användning, behandling och analysering av handlingar och andra upptagningar som anknyter till ett underrättelseuppdrag för att producera information som underrättelseuppdraget förutsätter och uppnå målet med underrättelseuppdraget. Undersökningen ska föregås av sådan granskning av upptagningar och handlingar som avses i 107 §, vilket gör att materialet inte längre borde innehålla material som bl.a. omfattas av förbud mot underrättelseinhämtning i den fas då upptagningarna undersöks.

Den krets som har rätt att undersöka upptagningar ska vara begränsad för att integritetsskyddet ska kunna säkerställas tillräckligt effektivt.

Underrättelseinhämtningens art förutsätter att kretsen av personer som undersöker upptagningar är större än den krets av personer som fattar beslut och utövar befogenheterna. Enligt 2 mom. ska upptagningar dessutom på förordnande av Huvudstabens underrättelsechef också få undersökas av en sakkunnig som står utanför militärunderrättelsemyndigheterna eller av en annan person som bistår vid informationsinhämtningen. Mängden material som kommer till

dessa personers kännedom begränsas av att de får undersöka upptagningar endast på förordnade av Huvudstabens underrättelsechef i en viss situation och för ett visst syfte. Den som har gett förordnandet ska svara för att personen i fråga har de kunskaper och färdigheter samt den erfarenhet som behövs för att uppdraget ska kunna utföras på korrekt sätt.

**109 §.** *Protokoll*. Enligt bestämmelsen ska en tjänsteman vid en militärunderrättelsemyndighet som använder en metod för underrättelseinhämtning upprätta ett protokoll eller ett annat motsvarande dokument över användningen av metoden för underrättelseinhämtning. Av protokollet ska också framgå vem som har granskat upptagningarna och vem som senare har undersökt dem. Det ska också framgå vem som får undersöka upptagningarna, även om någon egentlig undersökning av dem inte har gjorts.

Närmare bestämmelser om innehållet i protokollet utfärdas genom förordning av statsrådet.

Med ett annat motsvarande dokument ska avses ett dokument i en annan form än ett protokoll, i vilket kan ingå också annan information än registreringar. Till sina egenskaper ska dokumentet dock motsvara ett protokoll och av det ska framgå alla motsvarande uppgifter.

Protokollet och de uppgifter som noggrant har förts in i det möjliggör den övervakning av underrättelseverksamheten som avses i denna lag samt underrättelseombudsmannens laglighetsövervakning.

**110 §.** *Tystnadsplikt*. Enligt 1 mom. gäller i fråga om tystnadsplikt för tjänstemän som är anställda vid militärunderrättelsemyndigheterna vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet, någon annanstans i lag och nedan i detta kapitel.

Enligt första meningen i 23 § 1 mom. i lagen om offentlighet i myndigheternas verksamhet får den som är anställd hos en myndighet inte röja en handlings sekretessbelagda innehåll eller en uppgift som vore sekretessbelagd om den ingick i en handling. I 24 § föreskrivs om sekretessbelagda myndighetshandlingar. I 1 mom. 10 punkten i paragrafen föreskrivs om handlingar som gäller bl.a. militär underrättelseinhämtning, om det inte är uppenbart att utlämnandet av uppgifter ur dessa inte skadar eller äventyrar intressen som gäller landets försvar.

Enligt 2 mom. får tjänstemän som hör till en militärunderrättelsemyndighets personal inte röja uppgifter som avslöjar identiteten hos en person som har lämnat information konfidentiellt eller deltagit i en täckoperation inom den militära underrättelseinhämtningen, om röjandet av uppgifterna kan äventyra den persons säkerhet som har lämnat information konfidentiellt eller deltagit i en täckoperation, eller en närstående persons säkerhet. Tystnadsplikten gäller också om röjandet av uppgifterna om identiteten kan äventyra ett pågående eller framtida underrättelseuppdrag. Momentet ska också gälla den som sporadiskt lämnar ut konfidentiell information.

De uppgifter som avses i momentet är ytterst sensitiva och kan äventyra förutom en tjänsteman vid militärunderrättelsemyndigheterna också flera utomstående. Med anledning av detta ska de uppgifter som avses i momentet behandlas endast av vissa tjänstemän vid militärunderrättelsemyndigheterna, och de uppgifter som avses i momentet ska inte få hamna utanför denna krets av personer. Eftersom också andra personer än militärunderrättelsemyndigheternas tjänstemän kan vara med om att utföra ett underrättelseuppdrag i enlighet med denna lag i andra sammanhang, är det ändamålsenligt att föreskriva att tystnadsplikten också gäller dessa personer. Den andra meningen i momentet ska följaktligen gälla motsvarande personkrets som den om vilken föreskrivs i andra meningen i 1 mom.

I 3 mom. ska det föreskrivas om tystnadsplikten i situationer där röjandet av uppgifter om identiteten kan äventyra redan avslutad, pågående eller framtida informationsinhämtning. Eftersom underrättelseverksamhet är en långvarig verksamhet, som vissa personer under en mycket lång tid kan anknyta till, även om de emellanåt inte aktivt deltar i militär underrättelseverksamhet, ska tystnadsplikten vara långvarigare. Också den fara för liv eller hälsa som riktas mot personer med anknytning till militär underrättelseverksamhet kan konkretiseras först år efter att en underrättelseinsats har genomförts. Av denna anledning är det motiverat att förbudet mot att röja information om sådana personer ska vara omfattande.

Paragrafens 4 mom. ska gälla situationer där någon annan än en anställd vid en militärunderrättelsemyndighet utför uppgifter i samband med underrättelseinhämtning. Mest omfattande är denna persongrupp, om beväringar och reservister används. Vidare omfattar momentet övriga tjänstemän vid Försvarsmakten, vilka ska användas vid fullgörandet av ett underrättelseuppdrag. I de situationer som avses i 4 mom. ska de parter som deltar i ett underrättelseuppdrag alltid ledas och övervakas av militärunderrättelsemyndigheterna.

Med hänvisningen i momentet till paragrafens 1–3 moment ska andra parter än de som är anställda vid militärunderrättelsemyndigheterna i princip vara bundna av förbudet att röja information enligt offentlighetslagen.

I underrättelseverksamhet strävar man efter att ytterst noggrant skydda identiteten hos de parter som lämnar information. Med anledning av detta ska dessa uppgifter behandlas endast av ett litet antal tjänstemän vid militärunderrättelsemyndigheterna. I vissa situationer kan information om t.ex. någon som har lämnat ut uppgifter komma till någon annans kännedom än en tjänsteman vid militärunderrättelsemyndigheterna, såsom vid användningen av vissa reservister som förutsätts vid effektivering av en beredskapssituation. Också i dessa situationer är det ändamålsenligt att föreskriva om tystnadsplikt uttryckligen genom att i paragrafen hänvisa till paragrafens 2 mom.

I fråga om andra än reservister och värnpliktiga kan det vara ändamålsenligt att också meddela ett beslut om ett yppandeförbud till en sådan person. En sådan situation kan komma i fråga t.ex. vad gäller tolkar och utomstående tekniska sakkunniga.

Enligt 5 mom. ska tystnadsplikten gälla också efter det att ett anställningsförhållande till militärunderrättelsemyndigheterna har upphört. Med anställningsförhållande ska avses alla de situationer där en person inte längre anses stå i ett förhållande till militärunderrättelsemyndigheterna.

**111 §.** *Tystnadsrätt*. Enligt 1 mom. ska de som är anställda inom den militära underrättelseinhämtningen inte vara skyldiga att röja uppgifter om identiteten hos en person av vilken de i sitt anställningsförhållande har fått information konfidentiellt och inte heller om sekretessbelagda taktiska eller tekniska metoder. Tystnadsrätten ska gälla alla situationer, inklusive utfrågningar i domstol och andra utfrågningar samt situationer där t.ex. en annan myndighet eller en enskild part hör sig för om saken.

I 2 mom. ska det föreskrivas om tystnadsrätt för andra som deltar i militär underrättelseinhämtning än de som är anställda vid militärunderrättelsemyndigheterna. Momentet ska omfatta beväringar och reservister som eventuellt används vid militär underrättelseinhämtning samt parter som har bistått i ett underrättelseuppdrag inom militär underrättelseinhämtning, såsom de tolkar och tekniska sakkunniga som militärunderrättelsemyndigheterna använder.

**112 §.** *Tjänstetecken*. Enligt 1 mom. ska Huvudstaben fastställa ett tjänstetecken som militärunderrättelsemyndigheternas tjänstemän ska medföra vid tjänsteutövning. I den föreslagna lagen finns bestämmelser som förutsätter att ställningen inom myndigheten visas. Dylika är t.ex. kvarhållande av en försändelse för kopiering, om vilket ska föreskrivas i 56 §. Myndigheten ska i dessa fall kunna visa sin myndighetsställning så att en person som är föremål för en skyldighet får information om att det är fråga om en myndighet i överensstämmelse med denna lag och att ett förordnande av myndigheten gäller honom eller henne.

Enligt 2 mom. ska en tjänsteman vid en militärunderrättelsemyndighet vid behov kunna visa upp ett tjänstetecken vid utförandet av ett tjänsteuppdrag.

I princip behöver militärunderrättelsemyndigheterna inte meddela sin tjänsteställning. Vid militär underrättelseinhämtning bär tjänstemännen vid myndigheterna i princip inte uniform, för att en person som är föremål för en metod för underrättelseinhämtning inte ska fästa särskild uppmärksamhet vid dem. I en dylik situation ska en tjänsteman i princip inte ens ha tjänstetecknet med sig. Om man på förhand vet att den som är föremål för en åtgärd kommer att ges skyldigheter, är det mera motiverat att ha tjänstetecknet med sig. Skyldigheten att visa upp ett tjänstetecken ska begränsas till sådana situationer där det är möjligt utan att en åtgärd äventyras. Till exempel det yppande av tystnadsplikt som avses i motiveringarna till 1 mom. är inte möjligt utan att den person som är föremål för tystnadsplikten vet om att det är frågan om en tjänsteman.

När ett tjänstetecken visas upp ska det beaktas att en åtgärd som ska vidtas kan äventyras och avslöjas till följd av att tjänstetecknet visas.

I 3 mom. ska det föreskrivas om andra identifikationer som utvisar en tjänstemans ställning vid militärunderrättelsemyndigheterna än de som avses i 1 mom. En sådan identifikation ska godkännas och beslut om användningen av den fattas av Huvudstabens underrättelsechef. Behov av att använda en identifikation enligt momentet kan förekomma t.ex. i en situation där det av praktiska skäl är nödvändigt att uppge militärunderrättelsemyndigheternas myndighetsstatus för en tredje part, medan den måste hemlighållas för utomstående för att skydda verksamheten eller för att syftet med den ska uppnås.

Enligt 4 mom. ska en tjänsteman kunna identifieras. Bestämmelsen är av betydelse med tanke på rättsskyddet för den person som är föremål för åtgärden. Identifieringen av en tjänsteman kan genomföras t.ex. genom noggrann registrering av åtgärderna och vem som vidtagit dem.

**113 §.** *Förfarandet i domstol.* I paragrafen ska det föreskrivas om domstolsbehandling av en metod för underrättelseinhämtning.

Enligt 1 mom. ska ett tillståndsärende som gäller en metod för underrättelseinhämtning behandlas vid Helsingfors tingsrätt. Tingsrätten ska vara domför med ordföranden ensam. Sammanträdet ska kunna hållas även vid en annan tidpunkt och på en annan plats än vad som förskrivs om en allmän underrätts sammanträde.

De tillståndsärenden som gäller metoder för underrättelseinhämtning ska endast behandlas vid Helsingfors tingsrätt. Ett dylikt koncentrerat beslutsarrangemang gäller i den gällande lagstiftning för närvarande endast täckoperation av de hemliga metoder för inhämtande av information, vilka avses i 5 kap. i polislagen. Flera motiveringar kan anges som stöd för att koncentrera beslutsfattandet till en enda tingsrätt. Vid Helsingfors tingsrätt arbetar flera tingsdomare som koncentrerar sig på tvångsmedelsärenden. En kompetensanhopning av detta slag möjlig-

gör specialisering på tillståndsärenden som gäller metoder för underrättelseinhämtning samt på frågor som gäller anmälningar om användningen av metoder för underrättelseinhämtning. Det att Helsingfors tingsrätt har ett större antal anställda än andra underrätter ger också bättre möjligheter att med sammanträdesarrangemang försäkra sig om att den domare som har jour är förtrogen med behandlingen av ärenden som gäller metoder för underrättelseinhämtning. En koncentrering styrks dessutom av att antalet personer som känner till användningen av metoder för underrättelseinhämtning ska begränsas samt av genomförandet av de säkerhetsarrangemang som behövs.

Den bestämmelse som gäller en beslutsför sammansättning i domstolen samt sammanträdets tid och plats motsvarar i sak bestämmelsen om häktningsberättigad myndighet i 3 kap. 1 § 2 mom. i tvångsmedelslagen.

Enligt 2 mom. ska ett yrkande om användning av en metod för underrättelseinhämtning göras skriftligen. För ett yrkande som gäller användning av en metod för underrättelseinhämtning ska således gälla samma villkor som vad som föreskrivs i 3 kap. 3 § 1 mom. i tvångsmedelslagen.

I momentet ska det dessutom föreskrivas att ett yrkande som gäller användning 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 att behandlingen ska ske utan dröjsmål förutsätter att ett anhänggjort ärende som gäller en metod för underrättelseinhämtning så snabbt som möjligt ska delges den domare som avgör ärendet samt att en sammanträdestidpunkt ska fastslås för målet. Den förordnade tjänstemannen förutsätts vara så förtrogen med metoder för underrättelseinhämtning att han eller hon kan besvara frågor och motivera yrkandet.

I 3 mom. ska det föreskrivas att ärendet ska avgöras skyndsamt. Om domstolen inte åläggs att behandla ärendet skyndsamt kan användningen av metoder för underrättelseinhämtning mista sin betydelse, och i värsta fall leda till att det militära försvaret och den nationella säkerheten äventyras.

I momentet ska det föreskrivas att behandlingen också kan ske med anlitande av videokonferens eller någon annan lämplig teknisk metod för dataöverföring där de som deltar i behandlingen har sådan kontakt att de kan tala med och se varandra. Dataöverföringssätten vid behandlingen ska därmed vara desamma som för närvarande gäller vid hemligt inhämtande av information med stöd av 5 kap. 45 § 2 mom. i polislagen och vid hemliga tvångsmedel utgående från 10 kap. 43 § 2 mom. i tvångsmedelslagen. I takt med att tekniken och krypteringsteknikerna för datakommunikationsförbindelserna utvecklas kan det bli möjligt att också använda videoförhandling eller någon annan lämplig teknisk metod för dataöverföring vid behandlingen. Detta ska dock inte vara en förpliktande bestämmelse och vid behandlingen bör alltid beaktas vad som föreskrivs i 7 mom.

Enligt 4 mom. ska det i fråga om varje metod för underrättelseinhämtning finnas särskilda bestämmelser om innehållet i beslutet. Med den bestämmelse som gäller innehållet i beslutet uppmärksammas domstolen på att den i sitt beslut om användning av en metod för underrättelseinhämtning ska nämna de faktorer om vilka föreskrivs i detalj i denna lags bestämmelser om de beslut som gäller användningen av metoder för underrättelseinhämtning.

I sin bedömning av nämnda faktorer har domstolen enbart de uppgifter som militärunderrättelsemyndigheterna har meddelat domstolen att förlita sig på. Därför är det ytterst viktigt att

av motiveringarna såväl till tillståndsyrkandet som till det beslut som gäller tillståndet framgår de faktorer som lett till ansökan om och beviljandet av tillståndet och den juridiska slutledningen. Även om militärunderrättelsemyndigheterna handlar under tjänsteansvar framhäver en behandling som grundar sig på en enda målsägande betydelsen av att domaren aktivt använder sig av rätten till utfrågning och skyldigheten att ta reda på.

Enligt momentet ska beslutet meddelas omedelbart eller senast när behandlingen av sådana ärenden som gäller metoder för underrättelseinhämtning som anknyter till samma underrättelsehelhet har avslutats. Bestämmelsen ska förutsätta att domstolen i samband med delgivandet av ett beslut i ett ärende som gäller en metod för underrättelseinhämtning handlar på samma sätt som när ett beslut i ett häktningsärende avkunnas med stöd av 3 kap. 10 § 1 mom. i tvångsmedelslagen.

I 5 mom. ska det föreskrivas att 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 nämnda tjänsteman är närvarande också om användningen av metoden för underrättelseinhämtning redan har avslutats.

För att den militära underrättelseinhämtningens och domstolens resurser ska kunna användas ändamålsenligt och effektivt föreslås det att ärenden som gäller enbart byte av teleadresser och teleterminalutrustningar inte i alla situationer ska behöva behandlas vid ett sammanträde. Ett förenklat förfarande, som avses i momentet, ska kunna tillämpas enligt domstolens prövning och endast om tillståndet fortfarande är i kraft. Tillståndsärendet ska sålunda behandlas minst en gång i halvåret, 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 hot som allvarligt äventyrar den nationella säkerheten som utgjorde grund för användningen av metoden för underrättelseinhämtning i det tidigare beviljade tillståndet.

Med ett fall enligt den senare meningen i momentet anknyter samma slag av ändamålsenlighetsaspekter som i de situationer som avses i första meningen. Den senare meningen ska således gälla situationer där Huvudstabens underrättelsechef eller en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman tillfälligt har beslutat om användning av en metod för underrättelseinhämtning med stöd av 36 § 1 mom., 38 § 1 mom. eller 53 § 2 mom. samt situationer där en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman tillfälligt har beslutat om användning av en metod för underrättelseinhämtning med stöd av 29 § 1 mom. eller 31 § 1 mom.

I 6 mom. i paragrafen föreslås det att ett beslut i ett tillståndsärende inte ska få överklagas genom besvär. Klagan mot beslutet ska få anföras utan tidsbegränsning vid Helsingfors hovrätt. Klagan ska behandlas skyndsamt.

Till denna del motsvarar bestämmelsen 5 kap. 45 § 5 mom. i gällande polislag med den preciseringen att Helsingfors hovrätt ska nämnas som domstol för klagan.

I 7 mom. ska det föreskrivas att vid handläggningen av ett ärende som gäller en metod för underrättelseinhämtning ska särskild vikt fästas vid att sekretessen iakttas och att information-

en i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.

Ärendet ska enligt vad som föreslås vid behov kunna behandlas någon annanstans än i en domstol, till exempel i skyddspolisens lokaler. Det finns skäl att fästa särskilt avseende vid tystnadsplikten och datasekretessen. De viktigaste sekretessbestämmelserna ingår i lagen om offentlighet vid rättegång i allmänna domstolar (370/2007).

**114 §.** *Begränsning av partsoffentlighet i vissa fall*. Enligt 1 mom. har en person vars rättigheter eller skyldigheter saken gäller inte, trots vad som föreskrivs i 11 § i lagen om offentlighet i myndigheternas verksamhet, rätt att få vetskap om användningen av en metod för informationsinhämtning enligt denna lag förrän underrättelse enligt 86 § har getts. Han eller hon ska inte heller ha rätt till insyn för registrerade enligt personuppgiftslagen.

Avsikten med momentet är att lagstiftningsmässigt förtydliga situationen i förhållande till lagen om offentlighet i myndigheternas verksamhet och personuppgiftslagen.

I 11 § i lagen om offentlighet i myndigheternas verksamhet föreskrivs om en parts rätt att ta del av en myndighetshandling samt om de situationer då parten inte har rätt att få en handling. Enligt 1 mom. 1 punkten har en part inte rätt att få information ur en handling när utlämnande av uppgifter skulle strida mot ett synnerligen viktigt allmänt intresse. Ett synnerligen viktigt intresse är t.ex. intresset att hemlighålla en taktisk eller teknisk metod för militär underrättelseinhämtning.

Enligt momentet ska en person dock ha rätt att få de uppgifter som avses i 1 mom., om till honom eller henne har getts en sådan underrättelse som avses i 86 §.

**115 §.** *Närmare bestämmelser*. I paragrafen ska det föreskrivas om de frågor som det ska kunna föreskrivas närmare om genom förordning av statsrådet eller förordning av försvarsministeriet.

I 1 mom. föreslås att genom förordning av statsrådet får det utfärdas bestämmelser om 1) organiserandet av användningen och skyddandet av metoder för underrättelseinhämtning, 2) dokumenteringen av åtgärderna för övervakningen, 3) de redogörelser som ska lämnas för övervakningen av den militära underrättelseinhämtningen, 4) det förfarande som gäller överföring av en uppgift som ska lämnas ut för brottsbekämpning, 5) organiserandet av samarbetet mellan militärunderrättelsemyndigheterna och skyddspolisen, 6) organiserandet av samarbetet mellan militärunderrättelsemyndigheterna och andra myndigheter, 7) organiserandet av samordningen av den hemliga informationsinhämtningen och 8) organiserandet av samordningen av underrättelseverksamheten.

I 2 mom. föreslås att genom förordning av försvarsministeriet får det utfärdas bestämmelser om 1) organiserandet av övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen och 2) organiserandet av militärunderrättelsemyndigheternas internationella samarbete.

Av alla bestämmelser som gäller bemyndigande att utfärda förordning framgår att de har avgränsats till tekniska eller förfaringsmässiga omständigheter. Till exempel bestämmelsen om bemyndigande i 1 mom. 1-4 punkterna har sakligt samma innehåll som 5 kap. 65 § i polislagen och 10 kap. 67 § i tvångsmedelslagen.

Med beaktande av omständigheternas natur är det motiverat att bestämma om dem på förordningsnivå, eftersom det inte är fråga om en individs rättigheter och skyldigheter, varvid om saken borde föreskrivas i lag, utan om organiserandet av en myndighets interna verksamhet eller av verksamheten mellan myndigheterna.

**116 §.** *Ikraftträdande*. Lagen föreslås träda i kraft så fort som möjligt.

### 1.2 Lagen om försvarsmakten

**8 a §.** *Militär underrättelseverksamhet.* I paragrafen föreslås bestämmelser om den underrättelseverksamhet som hör till Försvarsmaktens ansvarsområde.

I lagens 2 kap. finns alla bestämmelser om den behörighet som behövs för att sköta de uppgifter inom Försvarsmakten som avses i 1 kap. eller hänvisningar till gällande lagar i vilka det föreskrivs om behörigheten samlade. Därför föreslås att det till kapitlet fogas en ny hänvisningsbestämmelse till den nya lagen om militär underrättelseverksamhet, i vilken det ska föreskrivas om syftet med Försvarsmaktens underrättelseverksamhet, dvs. militär underrättelseinhämtning, om myndigheternas uppgifter och befogenheter, beslutsfattande, tekniskt genomförande av underrättelseinhämtning samt om styrningen av underrättelseinhämtningen och övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen.

Syftet med militär underrättelseinhämtning är att inhämta och behandla information om yttre hot för att Försvarsmakten ska kunna utföra sina uppgifter enligt 2 § 1 mom. 1 a och 1 b punkten samt 1 mom. 3 och 4 punkten. Militär underrättelseinhämtning kan alltså inte bedrivas i sådana uppgifter inom Försvarsmakten som gäller givande av militär utbildning, styrning av den frivilliga försvarsutbildningen, främjande av försvarsviljan och deltagande i handräckning eller räddningsverksamhet.

### 1.3 Lagen om militär disciplin och brottsbekämpning inom försvarsmakten

**13 §.** *Huvudstabens behörighet att utfärda bestämmelser*. I paragrafen föreskrivs om de förmän som ska ha motsvarande disciplinära befogenheter som disciplinära förmän samt om huvudstabens skyldighet att meddela föreskrifter om detta.

Enligt förslaget ska det i paragrafen tas in en uttrycklig bestämmelse om att tjänstemän vid militärunderrättelsemyndigheten, dvs. Försvarsmaktens underrättelsetjänst och huvudstabens underrättelseavdelning, inte har i denna lag avsedda disciplinär förmans befogenheter. Detta innebär att nämnda tjänstemän inte kan utföra förundersökning eller utöva befogenheter i anslutning till förundersökning. De närmaste disciplinära förmän som är skyldiga att inleda förundersökning är i fortsättningen chefen för huvudstaben och försvarsmaktens operationschef.

Militärunderrättelsemyndigheten har dock inte prövningsrätt när det gäller hur och i vilket skede den meddelar den disciplinära förmannen om en misstanke om ett militärt brott som kommit till dess kännedom. En tjänsteman vid militärunderrättelsemyndigheten har tjänsteplikt att underrätta den behöriga disciplinära förmannen, åklagaren eller laglighetsövervakningen om ett sådant misstänkt lagstridigt förfarande av en tjänsteman vid militärunderrättelsemyndigheten som eventuellt uppfyller rekvisitet för militärt brott. Chefen för huvudstaben kan alltid inleda en förundersökning. Chefen för huvudstaben har också en lagstadgad övervakningsuppgift.

Militärunderrättelsemyndigheten ska enligt behov alltjämt kunna delta i förundersökningen av ett militärt brott i egenskap av sakkunnigmyndighet.

I paragrafens rubrik och i den sista meningen görs språkliga ändringar som förbättrar läsbarheten.

**27 §.** *Förrättande av förundersökning.* I paragrafen föreskrivs om förrättande av förundersökning i Försvarsmaktens truppförband. Skyldigheten att förrätta en förundersökning gäller även den militärunderrättelsemyndighet som är förundersökningsmyndighet, dvs. huvudstaben och Försvarsmaktens underrättelsetjänst.

Målet är att göra en tydlig skillnad mellan förundersökning och militär underrättelseinhämtning. I syfte att garantera en rättvis rättegång tas i paragrafen in ett nytt 3 mom. om att förundersökningen av ett brott som en tjänsteman vid Försvarsmaktens underrättelsetjänst misstänks för görs av huvudstaben. Bestämmelser om förrättande av förundersökning vid huvudstaben finns i 35–41 §. Bestämmelser om förundersökningen av ett brott som en civil tjänsteman vid militärunderrättelsemyndigheten misstänks för utfärdas särskilt.

Till övriga delar kvarstår paragrafens sakinnehåll oförändrat.

**36 §.** *Huvudstabens tjänstemän som sköter förundersökning*. I paragrafen föreskrivs om de tjänstemän vid huvudstaben som utför förundersökning och utövar de befogenheter som har samband med den. Enligt 1 mom. 1 punkten utövar försvarsmaktens assessor och en militärjurist de befogenheter som har föreskrivits för en polisman som hör till befälet och för en anhållningsberättigad tjänsteman, och enligt 2 punkten utövar överdetektiven och en yrkesmilitär som avses i lagen om försvarsmakten och som har förordnats till en förundersökningsuppgift eller en annan tjänsteman som är anställd vid försvarsmakten och har förordnats till uppgiften de befogenheter som har föreskrivits för en polisman och utredare.

Det föreslås att det inledande stycket i 1 mom. preciseras så att de som utför förundersökning och utövar de befogenheter som har samband med den uttryckligen ska vara tjänstemän vid huvudstabens juridiska avdelning. Regleringen motsvarar därmed nuvarande praxis. Avsikten är att även på lagnivå säkerställa att förundersökningen utförs av andra tjänstemän än de som förebygger och avslöjar brott eller sköter uppdrag inom den militära underrättelseverksamheten. I 1 mom. 2 punkten slopas hänvisningen till en tjänsteman som är anställd vid försvarsmakten som onödig, eftersom det av både paragrafens rubrik och det inledande stycket i 1 mom. framgår att det i bestämmelsen är fråga om tjänstemän vid huvudstaben.

I 2 mom. föreslås för tydlighetens skull en ny bestämmelse om att enskilda förhör och andra undersökningsåtgärder kan ges i uppdrag åt en utredare enligt 28 § 3 mom. som är anställd vid Försvarsmakten t.ex. i syfte att påskynda undersökningen eller trygga den förhördes rättsskydd. Förfarandet motsvarar nuvarande praxis.

Till övriga delar kvarstår paragrafens sakinnehåll oförändrat.

**86 §.** *Behörighet vid förebyggande och avslöjande av brott.* I paragrafen föreskrivs om Försvarsmaktens behörighet vid förebyggande och avslöjande av brott. I paragrafens 3 mom. finns en informativ hänvisning om att skyddspolisen sörjer för att ett sådant brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och ett sådant brott som äventyrar syftet med det militära försvaret reds ut.

I den regeringsproposition som gäller civil underrättelseinhämtning utökas skyddspolisens befogenheter att inhämta underrättelser och begränsas befogenheterna att utföra förundersökning. Eftersom det i förslagen till ändring av förundersökningslagen (1 §) och polisförvaltningslagen (10 §) i den nämnda propositionen föreslås att uppdrag för utredning av brott inte längre ska skötas av skyddspolisen, föreslås det att 3 mom. ändras så att centralkriminalpolisen i fortsättningen ska sörja för att det som avses i 1 mom. reds ut på det militära försvarets område.

Centralkriminalpolisens främsta uppgift är att förebygga och avslöja organiserad brottslighet och annan brottslighet av grövsta slag. Centralkriminalpolisen utreder i regel själv de brott som den avslöjat. Dessutom utreder centralkriminalpolisen annan brottslighet av grövsta slag som den fått kännedom om och särskilt brottsfall med samhällelig betydelse.

### 1.4 Lagen om verksamheten i den offentliga förvaltningens säkerhetsnät

**6 §.** *Tillhandahållare av nät- och infrastrukturtjänster.* I paragrafen föreskrivs att aktiebolaget Suomen Erillisverkot Oy och ett dotterbolag som Suomen Erillisverkot Oy separat bildat för detta ändamål och som helt och hållet ägs av nämnda bolag kan vara tillhandahållare av nät- och infrastrukturtjänster i säkerhetsnätet. I paragrafen föreskrivs om principerna för ordnandet av tjänsteproduktionen, vari det bl.a. ingår att administrativt, funktionellt och ekonomiskt avskilja säkerhetsnätsverksamheten från bolagets övriga verksamhet. I paragrafen konstateras dessutom att ett dotterbolag som Suomen Erillisverkot Oy separat bildat för det ändamål som avses i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät och som helt och hållet ägs av nämnda bolag inte får ha andra uppgifter eller funktioner och att det inte får ha som syfte att uppnå företagsekonomisk vinst.

Det föreslås att paragrafens 3 mom. ändras så att ett dotterbolag också får ha andra uppgifter än uppgifter i anslutning till säkerhetsnätsverksamheten, om så föreskrivs någon annanstans i lag. Härmed hänvisas t.ex. till uppgiften enligt lagen om militär underrättelseverksamhet att vara den som utför en koppling enligt 9 § 1 punkten i den lagen.

Uppgiften att utföra en koppling som underrättelseverksamheten förutsätter kan inte betraktas som en uppgift som hör till underrättelseverksamhetens tjänsteproduktion och därför ska det krav på avskiljande av verksamheten som avses i 2 mom. beaktas vid skötseln av uppgiften. Kravet gäller i synnerhet ekonomiskt avskiljande av uppgiften att utföra en koppling från bolagets övriga verksamhet. Administrativt och funktionellt avskiljande är inte ändamålsenligt. Det är kostnadseffektivt att uppgifterna att utföra en koppling görs av samma personer som sörjer för säkerhetsnätsverksamheten.

Till övriga delar kvarstår paragrafens sakinnehåll oförändrat.

I lagen om militär underrättelseverksamhet föreslås bestämmelser om Försvarsmaktens underrättelseverksamhet. För inriktning av underrättelseinhämtning som avser datatrafik ska Försvarsmaktens underrättelsetjänst 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 (64 §). Försvarsmaktens underrättelsetjänst ska ha rätt att med hjälp av automatisk databehandling i den datatrafik som överskrider Finlands gräns i kommunikationsnät inhämta information om en med avseende på ett underrättelseuppdrag väsentlig aktörs datatrafik samt behandla aktörens kommunikation (66 och 68 §).

Bestämmelser om genomförande av den koppling som behandlingen av tekniska data i datakommunikationen och underrättelseinhämtningen som avser datatrafik förutsätter ska finnas i 70 § i den nämnda lagen. Den som utför kopplingen verkställer de tillstånd av domstolen som gäller behandling av tekniska data och underrättelseinhämtning och styr den datatrafik som rör sig i den i tillståndet avsedda delen av kommunikationsnätet till Försvarsmaktens underrättelsetjänst. Den som utför kopplingen får ersättning för kostnaderna enligt självkostnadsvärde.

Bestämmelser om den som utför en koppling finns i definitionen i 9 § 1 punkten i lagförslaget om militär underrättelseinhämtning. Med den som utför en koppling avses en sådan tillhandahållare av nät- och infrastrukturtjänster som avses i 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät, dvs. aktiebolaget Suomen Erillisverkot Oy, eller ett dotterbolag som helt ägs av tillhandahållaren, dvs. Suomen Turvallisuusverkko Oy.

Ur Europadomstolens avgörandepraxis kan det härledas att underrättelsemyndigheten inte kan ha direkt och obegränsat tillträde till telekommunikationsnäten. Anslutningen till telekommunikationsnätet i enlighet med domstolens tillstånd ska därför göras av någon annan än underrättelsemyndigheten själv. Uppgiften anvisas någon som är oberoende av underrättelsemyndigheterna för att säkerställa att underrättelsemyndigheterna inte får mera omfattande tillträde till telekommunikationen än vad domstolens tillståndsbeslut medger. Genomförandet av en anslutning i enlighet med domstolens tillstånd, och till denna del verkställigheten av tillståndet, kan inte anses utgöra betydande utövning av offentlig makt, och därför kan uppgiften ges också till någon annan än en myndighet.

Säkerställandet av att kraven på rättssäkerhet och god förvaltning tillgodoses i den bemärkelse som avses i 124 § i grundlagen förutsätter att de allmänna förvaltningslagarna iakttas när kopplingen görs och att de som handlägger ärenden handlar under tjänsteansvar. På en person som är anställd av den som utför kopplingen tillämpas bestämmelserna om straffrättsligt tjänsteansvar när han eller hon utför uppgifter enligt lagen om militär underrättelseverksamhet (70 § i den lagen).

### 1.5 Inkomstskattelagen

**92 b §.** *Vittnesarvode, belöning för tips och arvode för användning av informationskälla.* Bestämmelser om skatteplikt för en fysisk persons inkomst finns i inkomstskattelagen. Systemet med inkomstskatt i Finland utgår från ett brett inkomstbegrepp, enligt vilket inkomster i pengar eller pengars värde är skattepliktiga, om det inte särskilt bestäms att de är skattefria. Normalt ska alltså arvoden som betalas t.ex. till informationskällor vara skattepliktig inkomst.

Paragrafen innehåller en specialbestämmelse om skattefrihet för vittnesarvode och belöning för tips. Skattepliktig inkomst är enligt 2 punkten inte ersättning eller arvode som en myndighet betalar eller förmedlar för information som har bidragit till att ett brott har förebyggts eller utretts, en gärningsman har gripits eller den nytta som ett brott har medfört har återfåtts. Bestämmelsen i fråga fogades till inkomstskattelagen i samband med revideringen av polislagen 2005.

I paragrafen föreslås en ny 3 punkt i vilken det föreskrivs att arvode som en myndighet betalar en informationskälla som avses i lagen om militär underrättelseverksamhet för inhämtande av uppgifter som är av betydelse för skötseln av underrättelseuppdrag inte är skattepliktig inkomst. Paragrafens rubrik ändras på motsvarande sätt. Till övriga delar kvarstår paragrafens sakinnehåll oförändrat.

I lagen om militär underrättelseverksamhet föreskrivs om användningen av informationskällor. Med användning av informationskällor avses enligt 46 § i den nämnda lagen annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av underrättelseuppdrag av någon annan än en myndighet, dvs. av en informationskälla. Militärunderrättelsemyndigheterna får be att en för ändamålet godkänd informationskälla som har lämpliga personliga egenskaper, har registrerats och har samtyckt till informationsinhämtning, inhämtar den information som avses ovan (styrd användning av informationskällor), om det med fog kan antas att styrd användning av informationskällor är av synnerlig vikt för erhållande av information med avseende på ett underrättelseuppdrag.

Till en registrerad informationskälla kan arvode betalas med stöd av 50 § i lagen om militär underrättelseverksamhet. Av grundad anledning kan arvode betalas även till en oregistrerad informationskälla. Särskilda bestämmelser ska gälla om skatteplikt för arvodet. Motsvarande bestämmelser om användning av informationskällor och det arvode som betalas inom civil underrättelseinhämtning finns i 5 kap. 40 § och 5 a kap. 24 § i polislagen.

För att säkerställa ett täckande skydd för informationskällan är det viktigt att identiteten på den person som gett information inte avslöjas i samband med beskattningen. För arvodets skattefrihet talar också den omständigheten att de arvoden som betalas till informationskällor är mycket sporadiskt förekommande och anspråkslösa. Det är alltså inte fråga om en sådan regelbunden inkomst för mottagaren som egentligen kan jämställas med lön.

Med beaktande av att belöning för tips blev skattefri i samband med revideringen av polislagen kan motsvarande skattebehandling betraktas som motiverad även i fråga om de arvoden som betalas vid användningen av informationskällor.

## 2 Närmare bestämmelser och föreskrifter

Genom förordning av statsrådet ska det på det sätt som anges i 115 § 1 mom. utfärdas bestämmelser om 1) organiserandet av användningen och skyddandet av metoderna för underrättelseinhämtning, 2) dokumenteringen av åtgärderna för övervakningen, 3) de redogörelser som ska lämnas för övervakningen av den militära underrättelseinhämtningen, 4) det förfarande som gäller överföring av en uppgift som ska lämnas ut för brottsbekämpningen, 5) organiserandet av samarbetet mellan militärunderrättelsemyndigheterna och skyddspolisen, 6) organiserandet av samarbetet mellan militärunderrättelsemyndigheterna och andra myndigheter, 7) organiserandet av samordningen av den hemliga informationsinhämtningen och 8) organiserandet av samordningen av underrättelseverksamheten.

Genom förordning av försvarsministeriet ska det på det sätt som anges i 115 § 2 mom. utfärdas bestämmelser om 1) organiserandet av övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen och 2) organiserandet av militärunderrättelsemyndigheternas internationella samarbete.

## 3 Ikraftträdande

Ett viktigt syfte med propositionen är att göra det möjligt att utveckla systemet för underrättelseinhämtning så att det motsvarar den förändrade omvärlden på så sätt att det kan produceras tillförlitlig och rättidig underrättelseinformation om hot mot Finlands säkerhetspolitiska miljö till stöd för det säkerhetspolitiska och militära beslutsfattandet. I Finlands närområde har Östersjöområdet fått större militärstrategisk betydelse och den militära aktiviteten i området har

ökat. 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 militära underrättelseinhämtningen har sämre möjligheter att producera rättidig underrättelseinformation. Inte bara den externa utan även den interna säkerhetspolitiska miljön har blivit allt mer utmanande och det har blivit svårare att förutse olika situationer.

I den allmänna motiveringen konstateras det att Finlands befogenheter att inhämta underrättelser är otidsenliga i internationell jämförelse. För att uppnå europeisk medelnivå krävs det en långsiktig utveckling av systemen och metoderna för underrättelseinhämtning. Detta utvecklingsarbete kan inte inledas innan de föreslagna nya befogenhetsbestämmelserna träder i kraft. Finlands förmåga till underrättelseinhämtning försvagas därför hela tiden i förhållande till andra stater så länge den förslagna regleringen inte är i kraft.

För att det ska vara möjligt att upprätthålla Finlands försvar och en fortlöpande förmåga att skydda den nationella säkerheten är det kritiskt viktigt att alla de metoder för underrättelseinhämtning som föreslås i propositionen kan användas av Försvarsmaktens militärunderrättelsemyndighet så snart som möjligt. Med hjälp av metoderna för underrättelseinhämtning kan Försvarsmakten upprätthålla den förmåga till underrättelseinhämtning som behövs vid uppföljningen av förändringar i omvärlden. En bristfällig förmåga till underrättelseinhämtning försvagar försvarets trovärdighet och tröskelförmåga.

Med information som inhämtats med de föreslagna befogenheterna stöds inte bara det militära försvaret utan även krishanteringsinsatserna. Bristfällig underrättelseinformation från målområdena för nuvarande och nya krishanteringsinsatser äventyrar säkerheten för de finländare som deltar i dem. De nya biståndsskyldigheterna i kombination med den allt svagare globala säkerhetsutvecklingen kan leda till ett behov för Finland att med kort förberedelse delta i militära insatser de närmaste åren.

De befogenheter som ingår i lagen om militär underrättelseverksamhet 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 och kraven på att den underrättelseinformation som behövs ska vara kontinuerlig och tidsenlig.

Förändringen i omvärlden har varit snabb och den fortgår alltjämt. För att säkerställa prestationsförmågan hos den för försvaret kritiskt viktiga militära underrättelseinhämtningen bör därför de föreslagna bestämmelserna i sin helhet sättas i kraft så snart som möjligt. Då kan man undvika att förmågan till militär underrättelseinhämtning försvagas alltför mycket i förhållande till Finlands snabbt förändrade säkerhetspolitiska miljö och möjliggöra den förmåga till tidig förvarning och den kännedom om omvärlden som Finlands försvarslösning behöver.

Av de skäl som anförts ovan föreslås lagarna träda i kraft så snart som möjligt.

De förslag till bestämmelser som ingår i lagförslag 1 och som gäller teknisk avlyssning (24 §), teknisk observation av utrustning (30 §), teleavlyssning av någon annan än en statlig aktör (32

§ 3 mom.), inhämtande av information i stället för teleavlyssning (33 §), teleövervakning som riktas mot någon annan än en statlig aktör (35 § 2 mom.), kopiering av försändelser (55 §) och underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer (68 §) förutsätter att grundlagen ändras och hänför sig således till den regeringsproposition som beretts vid justitieministeriet och som gäller en ändring av bestämmelserna om skydd för privatlivet i 10 § i grundlagen. Den propositionen ska behandlas i den ordning som anges i 73 § i grundlagen.

Om förslaget till ändring av grundlagen behandlas enligt huvudregeln, dvs. i s.k. normal grundlagsordning enligt 73 § 1 mom. i grundlagen, kan ovan nämnda bestämmelser eventuellt träda i kraft den 1 januari 2020. Om förslaget till ändring av grundlagen däremot behandlas i ett försnabbat förfarande enligt i 73 § 2 mom. i grundlagen kan ovan nämnda bestämmelser träda i kraft 2018 eller i början av 2019.

Om det inte anses finnas förutsättningar att ändra grundlagen genom brådskande förfarande och ändringen av grundlagen behandlas enligt normalt förfarande föreslås dock att de bestämmelser som inte förutsätter ändringar av grundlagen ska träda i kraft så snart som möjligt i normal lagstiftningsordning och att de inte tekniskt ska lämnas vilande över riksdagsvalet.

Propositionen har dessutom på det sätts om anges i avsnitt 6 ett nära samband med de regeringspropositioner som beretts vid inrikesministeriet och justitieministeriet och i vilka det föreslås bestämmelser om civil underrättelseinhämtning och övervakning av underrättelseverksamheten. Av denna orsak bör alla de ovan nämnda propositionerna träda i kraft samtidigt.

## 4 Förhållande till grundlagen och lagstiftningsordning

### 4.1 Inledning

Propositionen innehåller bestämmelser som är av betydelse för de grundläggande fri- och rättigheterna enligt grundlagen. Genom de befogenheter som används inom den militära underrättelseverksamheten ingriper utövarna i många fall i individens grundläggande fri- och rättigheter. De viktigaste i grundlagshänseende är de förslag som ger myndigheterna nya befogenheter som avser individen eller som i övrigt begränsar individens rättigheter eller näringsfriheten.

Även om användningen av olika metoder för underrättelseinhämtning ingriper i någon av de grundläggande fri- och rättigheterna, såsom skyddet för privatlivet enligt 10 § 1 mom. i grundlagen, försöker man vid tillämpningen av lagen om militär underrättelseverksamhet skydda övriga grundläggande fri- och rättigheter, såsom rätten till liv och personlig frihet enligt 7 § och de grunder för statsskicket som regleras i 1 kap., bl.a. statens suveränitet. Medborgarnas kollektiva trygghet liksom samhällets vitala funktioner och ett organiserat samhällsliv är så viktiga intressen att skydda, att det finns ett tungt vägande samhälleligt behov av och en med tanke på de grundläggande fri- och rättigheterna godtagbar grund för lagstiftningen om militär underrättelseverksamhet.

Information ska få inhämtas genom militär underrättelseverksamhet bara om sådana föremål som uttömmande har angetts i lagen. Det föreslås att det ska föreskrivas om dem så specificerat som det är möjligt med beaktande av underrättelseverksamhetens särdrag. Föremålen för underrättelseinhämtningen är oftast stater eller andra offentliga samfund som ligger utanför

grundlagsskyddet (RP 309/1993 rd och GrUU 9/2015 rd). Också metoderna för underrättelseinhämtning föreslås bli reglerade så exakt som möjligt och noggrant avgränsade.

Eftersom underrättelseinhämtning kan utföras endast av en myndighet som svarar för den nationella säkerheten, föreslås det att uppgiften enligt lag ska anförtros enbart militärunderrättelsemyndigheterna, dvs. Huvudstaben och Försvarsmaktens underrättelsetjänst.

De metoder för informationsinhämtning som föreslås i propositionen är till övervägande del sådana som i andra sammanhang har reglerats med grundlagsutskottets medverkan. Därmed har utvecklingen vad gäller de grundläggande bestämmelserna kunnat beaktas i propositionen.

Militärunderrättelsemyndigheten får, när tjänsteutövningen så kräver, ingripa i medborgarnas grundläggande fri- och rättigheter. Europadomstolen har ansett (Liberty m.fl. mot Förenade kungariket), att förfaranden i fråga om underrättelseinhämtning som avser datatrafik måste regleras tillräckligt exakt i lag. I förslaget till lag om militär underrättelseverksamhet föreskrivs det så noggrant som möjligt om myndighetens befogenheter och på ett sådant sätt, att användningen av befogenheter är tillåtna endast i den omfattning uppgiften kräver.

De befogenheter att ingripa i medborgarnas grundläggande fri- och rättigheter som ingår i den föreslagna lagen tillfaller endast tjänstemän som handlar under tjänsteansvar och som också är ansvariga för de reservister som utför biträdande uppdrag på deras begäran. Förslagen till bestämmelserna om befogenheter ska granskas som en helhet där också den övriga lagstiftning som föreslagits ingår.

Lagförslagen bör dessutom bedömas utifrån bestämmelserna om yttrandefrihet i 12 §, egendomsskydd i 15 §, rättsskydd i 21 §, ansvar för ämbetsåtgärder i 118 § och överföring av förvaltningsuppgifter på andra än myndigheter i 124 §. Lagförslagen bör dessutom granskas med hänsyn till de allmänna kriterierna för begränsning av de grundläggande fri- och rättigheterna (RP 1/1998 rd, GrUB 25/1994 rd)

### 4.2 Förslagen till bestämmelser om metoder för underrättelseinhämtning med hänsyn till bestämmelserna om de grundläggande fri- och rättigheterna

*Skydd för privatlivet*

I 10 § i grundlagen föreskrivs om skydd för privatlivet. Utgångspunkten för bestämmelsen är att individen har rätt att leva sitt liv utan godtyckligt eller obefogat ingripande från myndigheter eller andra utomstående. Bestämmelsen tryggar rätten till förtrolig kommunikation för var och en utan att utomstående obehörigen får kännedom om innehållet i förtroliga meddelanden som personen skickar eller tar emot. Detta innebär ett skydd t.ex. mot att brev eller andra förslutna försändelser öppnas eller förstörs och mot att samtal avlyssnas eller bandas. Bestämmelsen skyddar inte endast sändaren, utan det är fråga om en grundläggande rättighet för bägge parter. Utöver innehållet i meddelandet skyddar grundlagens bestämmelser också identifieringsuppgifterna för sändare och mottagare och andra uppgifter som kan ha betydelse för bevarandet av förtroligheten.

I 10 § 3 mom. i grundlagen föreskrivs det att det genom lag kan bestämmas om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna ska kunna tryggas eller för att brott ska kunna utredas. Genom lag kan det också bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som

äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång och säkerhetskontroll samt under frihetsberövande.

De här möjligheterna att begränsa skyddet av förtroliga meddelanden har i samband med reformen av de grundläggande rättigheterna avsetts vara en uttömmande förteckning (RP 309/1993 rd, s. 57). Bestämmelsen i 10 § 3 mom. i grundlagen nämner t.ex. Inte, med avvikelse från artikel 8 i Europakonventionen, den nationella säkerheten som ett sådant intresse som skulle berättiga till att lagstifta om begränsningar i hemligheten i fråga om förtroliga meddelanden.

Avsikten med grundlagsregleringen om hemlighet i fråga om förtroliga meddelanden är i första hand att mot utomstående skydda innehållet i ett meddelande som är avsett att vara förtroligt. Grundlagen tryggar var och en rätt till förtrolig kommunikation utan att utomstående orättmätigt kan få vetskap om innehållet i de förtroliga meddelanden som en person har sänt eller tagit emot. Detta innebär ett skydd t.ex. mot att brev eller andra förslutna försändelser öppnas eller förstörs och mot att samtal avlyssnas eller bandas. Regleringen skyddar inte bara avsändaren, utan det handlar om en grundläggande rättighet för båda parterna i kommunikationen (RP 309/1993 rd, s. 57, GrUU 28/2000 rd, s. 3, GrUU 30/2001 rd, s. 2, GrUU 54/2001 rd, s. 4, GrUU 13/2003 rd, s. 5, GrUU 9/2004 rd, s. 3–4, GrUU 10/2004 rd, s. 4–5, GrUU 16/2004 rd, s. 6, GrUU 59/2006 rd, s. 2, GrUU 19/2008 rd, s. 3).

Bestämmelsen skyddar inte innehållet i en vanlig diskussion på höravstånd som kan uppfattas med hörselsinnet, men avlyssnande av en diskussion som är avsedd att vara förtrolig med tekniska hjälpmedel innebär en begränsning i skyddet för hemligheten i fråga om förtroliga meddelanden (RP 309/1993 rd, s. 57, GrUU 11/2005 rd, s. 5, GrUU 36/2002 rd, s. 6, GrUU 2/1996 rd, GrUU 5/1999 rd, s. 4).

Bestämmelserna om grundläggande fri- och rättigheter skyddar fysiska personer och juridiska personer indirekt. Staten och andra offentliga samfund lämnas utanför skyddet för de grundläggande fri- och rättigheterna. Kommunikationen i en främmande stats myndighetsorganisation åtnjuter inte skydd för hemligheten i fråga om förtroliga meddelanden. För att upptäcka sådan kommunikation kan det dock vara nödvändigt att ingripa i hemligheten i fråga om förtroliga meddelanden. I fråga om kommunikation i samband med yrkesverksamhet är det möjligt att kommunikationen, med hänsyn till verksamhetens karaktär och till att parterna i kommunikationen är medvetna om att meddelandena lagras, inte omfattas av skyddet för hemligheten i fråga om förtroliga meddelanden, även om personer i och för sig också kan förmedla förtroliga meddelanden mellan sig i den kommunikationen (tele- och datakommunikation i samband med trafikledning, GrUU 62/2010 rd).

*Identifieringsuppgifter för förtroliga meddelanden*

Utöver innehållet i meddelandet skyddar grundlagens bestämmelser också identifieringsuppgifterna för sändare och mottagare och andra uppgifter som kan ha betydelse för bevarandet av förtroligheten. Identifieringsuppgifterna för ett meddelande har i grundlagsutskottets etablerade praxis ansetts ligga utanför kärnområdet för den grundläggande fri- och rättighet som skyddar hemligheten i fråga om förtroliga meddelanden.

Bestämmelser som inkräktar på skyddet för hemligheten i fråga om identifieringsuppgifter ska uppfylla de allmänna begränsningsförutsättningarna för grundläggande fri- och rättigheter (GrUU 62/2010 rd, s. 4, GrUU 23/2006 rd, s. 3, GrUUL 7/1997 rd). I grundlagsutskottets praxis har det på denna grund ansetts möjligt att rätten att få identifieringsuppgifter vid utred-

ning av brott inte binds vid vissa typer av brott, om regleringen i övrigt uppfyller de allmänna kraven på begränsningar av de grundläggande fri- och rättigheterna (GrUU 29/2008 rd, s. 2, GrUU 11/2005 rd, s. 4, GrUU 9/2004 rd, s. 4, GrUU 26/2001 rd, s. 3, GrUU 37/2002 rd, s. 3, GrUU 7/1997 rd). Regleringen ska dock i det fallet begränsas till att gälla brott som äventyrar individens eller samhällets säkerhet eller hemfriden eller som till svårhetsgraden kan jämställas med dem (GrUU 66/2010 rd, s. 7, GrUU 67/2010 rd, s. 4).

Grundlagsutskottet har dock efter EU-domstolens dom i ärendet Digital Rights Ireland bedömt att i praktiken kan identifieringsuppgifter som ansluter 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). Det är ännu inte möjligt att utifrån grundlagsutskottets senaste utlåtandepraxis entydigt avgöra vilka skillnader denna nya bedömning kan leda till jämfört med de tidigare tolkningarna, som stödde sig på de allmänna begränsningsförutsättningarna för grundläggande fri- och rättigheter. EU-domstolen har upprepat sina observationer vad gäller sammanställande och kombinering av uppgifter i ärendet Digital Rights Ireland i sitt avgörande i ärendet Tele2 Sverige AB.

*Skydd av 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 militära underrättelseinhämtningen hanteras också personuppgifter. I den personuppgiftslag för Försvarsmakten som är under beredning föreslås det att behandling av personuppgifter inom den militära underrättelseinhämtningen ska regleras i den föreslagna lagen och att bestämmelser om Försvarsmaktens behandling av personuppgifter ska ingå i den. Förslaget sammanhänger med totalrevideringen av den finska dataskyddslagsstiftningen, som ska göras på grund av Europeiska unionens lagstiftning som gäller dataskydd.

Parallellt med den föreslagna lagen om behandling av personuppgifter inom försvarsmakten ska också lagen om behandling av personuppgifter i brottmål och i samband med upprätthållandet av den nationella säkerheten tillämpas (RP /2018), som har föreslagits ingå som en allmän del i dataskyddslagstiftningen. På tillämpningsområdet för den helhet som dessa lagar bildar ska EU:s dataskyddsförordning och den föreslagna allmänna dataskyddslagen inte alls tillämpas.

Propositionen med förslag till lag om Försvarsmaktens behandling av personuppgifter och vissa andra lagar som har samband med den ska enligt planerna överlämnas till riksdagen vid

en tidpunkt som gör att den kan behandlas samtidigt med propositionen om lagstiftningen om underrättelseverksamhet.

I lagen om Försvarsmaktens behandling av personuppgifter ska det på ett heltäckande sätt och i detalj föreskrivas om register som gäller militär underrättelseinhämtning, deras användningsändamål, utlämnande av personuppgifter till en annan stat och till internationella organisationer, Försvarsmaktens rätt att få personuppgifter för att utföra militärunderrättelseuppdrag och om utplånande av personuppgifter i registren.

*Hemfrid*

Vars och ens privatliv är tryggat enligt 10 § 1 mom. i grundlagen. Enligt paragrafens 3 mom. kan det genom lag bestämmas om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna ska kunna tryggas eller för att brott ska kunna utredas.

Den hemfrid som tryggas i grundlagen omfattar i princip alla slag av utrymmen som används för permanent boende (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). Den sfär som skyddas av hemfriden definieras således inte på samma sätt i grundlagen som i t.ex. strafflagen.

De metoder för underrättelseinhämtning som är av betydelse med avseende på 10 § 1 mom. i grundlagen är systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, täckoperation, bevisprovokation genom köp och platsspecifik underrättelseinhämtning.

Ingen av de ovan nämnda metoderna får riktas mot utrymmen som används för stadigvarande boende. Det är tillåtet att använda metoderna täckoperation och bevisprovokation genom köp i en bostad endast om tillträde till eller vistelse i bostaden sker under aktiv medverkan av den som använder bostaden. Dessa metoder riktar sig därmed inte mot kärnområdet för det tryggande av hemfriden som avses i grundlagen. Utgångspunkten är att ingen av de nämnda metoderna för underrättelseinhämtning heller får riktas mot en bostad utomlands. Det kan emellertid visa sig omöjligt eller bereda orimligt stora svårigheter att få reda på bostadens användningsändamål, särskilt i mindre utvecklade länder.

De nämnda metoderna för underrättelseinhämtning kan därmed inte anses vara problematiska med avseende på tryggandet av hemfriden enligt 10 § 1 mom. i grundlagen.

*Meddelandesekretess*

I bestämmelserna om metoderna inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, optisk observation, teknisk spårning, täckoperation, bevisprovokation genom köp och platsspecifik underrättelseinhämtning har hänsyn tagits till de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna. Av denna orsak och med beaktande av att metoderna i fråga måste anses ingripa i hemligheten i fråga om förtroliga meddelanden och identifieringsuppgifterna i väldigt liten omfattning, kan de anses vara oproblematiska med avseende på 10 § 2 mom. i grundlagen.

Det föreslås att bestämmelser om kvarhållande av en försändelse för kopiering ska tas in i 57 § i lagförslag 1. Eftersom kvarhållande av en försändelse i motsats till kopiering av den inte in-

nebär en kränkning av brevhemligheten eller hemligheten i fråga om andra förtroliga meddelanden, har kvarhållande av en försändelse för kopiering betraktats som oproblematisk med avseende på de grundläggande fri- och rättigheterna.

Radiosignalspaning och underrättelseinhämtning som avser en främmande stats datatrafik får enligt 59 § 3 mom. och 61 § 3 mom. i lagförslag 1 inte gälla någon annan än en statlig aktör. Dessa metoder för underrättelseinhämtning är inte problematiska med avseende på tryggandet av meddelandehemligheten enligt 10 § i grundlagen. Radiosignalspaning utomlands får också riktas mot någon annan än en statlig aktör (63 § i lagförslag 1). I internationell verksamhet, t.ex. vid en militär krishanteringsinsats, kan det uppstå situationer där ett hot som inte har statligt ursprung, t.ex. terrorism, riktas mot Försvarsmakten. Dessutom är det inte nödvändigtvis möjligt att i alla situationer utnyttja teleavlyssning utomlands. I de situationer som nämns ovan kan det vara motiverat att rikta radiosignalspaning mot någon annan än en statlig aktör för att reda ut innehållet i ett meddelande. Radiosignalspaningen ska avbrytas omedelbart och de anteckningar och upptagningar den resulterat i ska utplånas, om den riktar sig mot någon annan än en statlig aktör.

För inriktning av underrättelseinhämtning som avser datatrafik ska Försvarsmaktens underrättelsetjänst ha rätt att samla in och lagra tekniska data om datatrafiken och med hjälp av automatisk databehandling behandla dem för statistisk analys. Behandlingen av de inhämtade data gäller inte meddelandenas innehåll utan endast tekniska data om kommunikationen. Med hjälp av resultatet kan underrättelseinhämtningen inriktas på enbart de delar av kommunikationsnätet där för underrättelseuppdraget viktig kommunikation försiggår.

Eftersom informationsinhämtningen endast kortvarigt gäller identifieringsuppgifter eller andra tekniska uppgifter om datatrafiken och militärunderrättelsemyndigheten inte har tillgång till tekniska uppgifter om enskilda meddelanden, kan myndigheten inte på det sättet få uppgifter om fysiska personer som är parter i kommunikationen. Behandlingen av tekniska uppgifter är därmed inte problematiska med avseende på det grundlagsfästa skyddet för meddelandehemligheten.

Metoderna teknisk avlyssning, teknisk observation av utrustning, teleavlyssning och inhämtande av information i stället för teleavlyssning, teleövervakning, kopiering som riktas mot ett meddelande och inriktning av underrättelseinhämtning som avser datatrafik kan anses vara ett betydande ingrepp i det skydd av förtroliga meddelanden som tryggas genom 10 § 2 mom. i grundlagen, utom när informationsinhämtningen avser kommunikationen i en främmande stats militära organisation eller annan myndighetsorganisation.

Även om teleövervakning tidigare har ansetts vara ett mindre ingrepp i skyddet för förtroliga meddelanden än teleavlyssning, kan identifieringsuppgifterna för elektroniska meddelanden och möjligheten att samla in och sammanställa dem vara till den grad problematiska med avseende på integritetsskyddet att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett mer allmänt plan fästa vikt också vid hur betydelsefulla begränsningarna är (GrUU 18/2014 rd, s. 6). Vid en konstitutionell granskning av underrättelseinhämtning som avser datatrafik bör man å andra sidan beakta att redan möjligheten att samla in uppgifter om datatrafik utgör ett ingrepp i integritetsskyddet (målen Klass mot Tyskland, Liberty m.fl. mot Förenade Kungariket).

Det är med stöd av 10 § 3 mom. i grundlagen inte möjligt att föreskriva om sådana begränsningar av meddelandehemligheten vars syfte är att avvärja eller utreda ett enskilt brott, utan

det är i större utsträckning fråga om inhämtande av nödvändig information om allvarliga yttre hot som Försvarsmakten behöver för att utföra sina lagfästa uppgifter.

Om verksamheten riktas mot någon annan än en statlig aktör blir det följaktligen möjligt att föreskriva om inhämtande av information i vanlig lagstiftningsordning med hjälp av metoderna teknisk avlyssning, teknisk observation av utrustning, teleavlyssning och inhämtande av information i stället för teleavlyssning, teleövervakning, kopiering av en försändelse och underrättelseinhämtning som avser datatrafik för att få information om militär verksamhet eller annan sådan verksamhet som allvarligt hotar den nationella säkerheten bara med stöd av den nya begränsningsgrunden för inhämtande av information som föreslås i 10 § 4 mom. i grundlagen och under förutsättning att bestämmelserna uppfyller de allmänna villkoren för begränsning av de grundläggande fri- och rättigheterna. Den nya begränsningsgrunden gör att det inte är möjligt att föreskriva om en allmän, ospecificerad och heltäckande spårning av datatrafik.

Europeiska domstolen för de mänskliga rättigheterna har ansett begränsningen av hemligheten i fråga om förtroliga meddelanden problematiskt med avseende på nödvändighet och lagenlighet, bl.a. när det gäller obegränsade befogenheter för underrättelsemyndigheterna att göra intrång i förtroliga meddelanden (Zakharov mot Ryssland). Också inom unionsrätten förutsätts det att informationsinhämtning ska grunda sig på mål som är godtagbara utifrån systemet för de grundläggande fri- och rättigheterna på ett sådant sätt att informationsinhämtningen inte gör oproportionella intrång i skyddet för privatlivet eller kränker unionsrättens centrala innehåll. I Europeiska unionens domstols rättspraxis har det särskilt betonats att informationsinhämtningen ska vara tillräckligt riktad och specificerad (avgörandena Digital Rights Ireland och Schrems).

Myndigheternas allmänna tillträde till innehållet i ett meddelande är en förbjuden kränkning av kärnområdet i skyddet för privatlivet och i fråga om ett regelsystem med stöd av vilket myndigheterna ges en allmän tillgång till innehållet i elektronisk kommunikation måste betraktas som ett synnerligen allvarligt ingrepp i det centrala innehållet i en grundläggande rättighet som garanteras i artikel 7 om respekt för privatlivet och familjelivet i stadgan om de grundläggande rättigheterna (Schrems, punkt 94, se även domen mot Digital Rights Ireland m.fl., C 293/12 och C 594/12, EU:C:2014:238, punkt 39).

*Rörelsefrihet*

I 9 § i grundlagen föreskrivs om rörelsefrihet. Finska medborgare samt utlänningar som lagligen vistas i landet har rätt att röra sig fritt inom landet och att där välja bostadsort. Begränsning av rörelsefriheten ska bygga på lag. Vid bedömning av om begränsningar ska tillåtas bör hänsyn tas också till artikel 2 i tilläggsprotokoll 4 till Europeiska konventionen om skydd för de mänskliga rättigheterna. Enligt dess 3 stycke kan utövandet av rätten att röra sig fritt inte underkastas andra inskränkningar än sådana som är angivna i lag och som är nödvändiga i ett demokratiskt samhälle.

De metoder för underrättelseinhämtning som är av betydelse med avseende på 9 § i grundlagen är inhämtande av basstationsuppgifter, systematisk observation, optisk observation och teknisk spårning. Dessa metoder innebär relativt små ingrepp i rörelsefriheten i förhållande till vilken nödvändig begränsningsgrund den nationella säkerheten utgör i ett demokratiskt samhälle. Därmed anses bestämmelserna om metoderna i fråga inte vara problematiska med avseende på rörelsefriheten.

*De allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna*

*Nödvändighet*

En begränsning av skyddet för förtroliga meddelanden måste enligt det föreslagna nya 10 § 4 mom. i grundlagen vara nödvändig. Denna förutsättning följer också av de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna.

Syftet med militär underrättelseverksamhet ska vara att inhämta information om yttre hot för att sköta de uppgifter Försvarsmakten enligt bestämmelserna i lagen om försvarsmakten har när det gäller att försvara rikets självständighet och territoriella integritet.

Vid bedömning av lagförslagets nödvändighet bör det beaktas att de föreslagna nya metoderna för underrättelseinhämtning får användas för att inhämta information bara om sådana föremål som uttömmande redovisas i lagen (4 § i lagförslag 1). Föremålen för militär underrättelseinhämtning anges på ett uttömmande sätt, vilket motsvarar kraven i Europadomstolens rättspraxis. Det anses t.ex. inte att enbart ett omnämnande i lag om att hemliga befogenheter får användas för att skydda den nationella säkerheten räcker inte för att uppfylla kravet på förutsebarhet (Zakharov mot Ryssland). Det kan å andra sidan inte heller förutsättas att det i en nationell lag exakt och uttömmande ska anges alla sådana situationer där myndigheterna får använda hemliga befogenheter. En bestämmelse i lag enligt vilken grunden för användning av hemliga befogenheter är ett militärt hot ska t.ex. anses uppfylla kravet på förutsebarhet enligt människorättskonventionen (Szabó och Vissy mot Ungern, Kruslin mot Frankrike, Huvig mot Frankrike). Informationsinhämtning om sådana föremål är nödvändig för att Finland ska kunna observera sin yttre säkerhetspolitiska omgivning och för att Försvarsmakten ska kunna fullgöra sina lagfästa uppgifter när det gäller att upprätthålla och utveckla försvarsberedskapen. Genom en informationsinhämtningsmetod får information inhämtas endast om sådan verksamhet som till sin natur är militär och som allvarligt hotar den nationella säkerheten (Kopp mot Tyskland, Kruslin mot Frankrike och Huvig mot Frankrike).

Information för inhämtas genom underrättelseinhämtningsmetoderna om sådan verksamhet som specificeras i 4 § 1 mom. i lagförslag 1, om verksamheten till sin art är militär. Det förutsätts i bestämmelsen, att föremålen ska ha anknytning till verksamhet som utförs av militärt organiserade trupper eller verksamhet som anknyter till militära maktmedel eller som kan jämställas med verksamhet som utövas med trupper och vapenmakt. Inhämtande av information om sådan verksamhet som avses i bestämmelsen och som till sin art är militär förutsätter inte att verksamheten utgör ett direkt allvarligt hot mot den nationella säkerheten.

Dessutom får information enligt 4 § 2 mom. i den föreslagna lagen inhämtas om en främmande stats verksamhet eller annan sådan verksamhet som kan äventyra det finska försvaret eller samhällets vitala funktioner. Med en främmande stats verksamhet eller annan sådan verksamhet som kan äventyra det finska försvaret avses t.ex. verksamhet som är så omfattande att den äventyrar Finlands möjligheter att fungera effektivt i en krissituation. Sådan verksamhet kan vara t.ex. ett omfattande och långvarigt angrepp mot datanät för att lamslå Finlands energiförsörjningssystem och som leder till att samhället inte kan fungera och försvagar försvarsberedskapen.

Sådana vitala funktioner som avses i 4 § 2 mom. i lagförslaget är bl.a. statens ledning, internationell verksamhet, upprätthållande av den interna säkerheten och en fungerande ekonomi och infrastruktur. Verksamhet som äventyrar dessa är t.ex. verksamhet vars syfte är att i betydande grad försvaga eller lamslå funktionerna. Med verksamhet som hotar samhällets vitala funktioner enligt momentet avses därmed verksamhet som allvarligt hotar den nationella säkerheten. Om föremålet för en metod för underrättelseinhämtning är någon annan än en främ-

mande stat och om den riktar sig mot skyddet för förtroliga meddelanden, får metoden användas i sådan informationsinhämtning som avses i 4 § 2 mom. bara om verksamheten allvarligt hotar den nationella säkerheten.

Varje punkt i 4 § 1 mom. ska kunna härledas ur ett eller flera intressen som springer ur behovet av skydd mot militär verksamhet. Bestämmelserna bedöms därmed uppfylla förutsättningarna i det föreslagna nya 4 mom. i grundlagens 10 §. Bestämmelserna om föremål för underrättelseinhämtning kan inte anses problematiska med avseende på skyddet för privatlivet. De bedöms också uppfylla de accentuerade kraven på nödvändighet och förutsebarhet.

*Exakt och noggrann avgränsning*

De allmänna förutsättningarna för användningen av underrättelseinhämtningsmetoder finns samlade i 11 § i den föreslagna lagen om militär underrättelseverksamhet (Amann mot Schweiz, Kopp mot Tyskland, Kruslin mot Frankrike, Huvig mot Frankrike). En allmän förutsättning för användning av underrättelseinhämtningsmetoderna är att användningen med fog kan antas ge information som behövs i underrättelseuppdraget. Det är fråga om en motiverad förväntning om att verksamheten ska ge resultat.

Eftersom metoderna teknisk avlyssning, teleavlyssning av någon annan än en statlig aktör, inhämtande av information i stället för teleavlyssning, teleövervakning av någon annan än en statlig aktör, kopiering av en försändelse och underrättelseinhämtning som avser någon annans än en statlig aktörs datatrafik kan innefatta betydande intrång i en enskilds skyddade rättsgoda, är en ytterligare förutsättning för användning av dessa metoder att de får användas för inhämtande av information endast om verksamheten allvarligt hotar den nationella säkerheten och inte är militär till sin art.

Det föreskrivs också om särskilda förutsättningar för användningen av underrättelseinhämtningsmetoderna och det föreskrivs om dessa förutsättningar i samband med var och en av metoderna i fråga (Amann mot Schweiz, Kopp mot Tyskland, Kruslin mot Frankrike, Huvig mot Frankrike). Av bestämmelserna om befogenheter framgår vad som är tillåtet vid utövandet av befogenheterna och vilka förfaranden som ska tillämpas, vad ett yrkande eller ett beslut ska innehålla, vem som fattar beslut om underrättelseinhämtningen, tillstånd att inhämta underrättelser, hur länge ett beslut eller ett förordnande gäller, eventuella förbud mot avlyssning, optisk observation, kopiering eller underrättelseinhämtning liksom om underrättelse om användning av en metod för underrättelseinhämtning.

Med undantag av metoderna platsspecifik underrättelseinhämtning, kopiering, radiosignalspaning och underrättelseinhämtning som avser datatrafik motsvarar de föreslagna metoderna för underrättelseinhämtning de hemliga metoder för informationsinhämtning som polisen har rätt att använda för att för att förhindra eller avslöja brott eller för att avvärja risken för brott. I motsats till polisens hemliga metoder för informationsinhämtning förutsätter inte militärunderrättelsemyndigheternas befogenheter för informationsinhämtning någon konkret och specificerad misstanke om brott. Användningsändamålen och förutsättningarna för användning av underrättelseinhämtningsmetoder avviker på grund av underrättelseverksamhetens karaktär på ett avgörande sätt från ändamålen och förutsättningarna för användning av de nuvarande hemliga informationsinhämtningsmetoderna. Upprätthållandet av allmän ordning och säkerhet har i lagstiftningen anförtrotts polisen. I princip är det endast i undantagsfall som uppgifter och befogenheter som hör till polisen åläggs någon annan myndighet, och det förutsätts också att det finns särskilda grunder för en sådan åtgärd. Grundlagsutskottet har i tidigare utlåtanden påpekat att ett likadant lagfäst bemyndigande för andra myndigheter att göra intrång i de

grundläggande fri- och rättigheterna som det som polisen har inte utan vidare är förenligt med det nödvändighetskrav som ingår i förutsättningarna (se GrUU 67/2016 rd, GrUU 10/2016 rd, s. 3, GrUU 49/2014 rd, s. 2, GrUU 37/2002 rd, s. 1-2 och GrUU 2/1996 rd, s. 3).

Det finns inte några bestämmelser i grundlagen om vilka myndigheter som kan ges befogenheter. Vid bedömningen av bestämmelser om myndigheters befogenheter har grundlagsutskottet utgått från att bestämmelserna ska vara av betydelse med tanke på rättsstatsprincipen i 2 § 3 mom. i grundlagen (se GrUU 51/2006 rd, s. 2). Enligt momentet ska all utövning av offentlig makt bygga på lag, och lag ska noggrant iakttas i all offentlig verksamhet. Utgångspunkten är att den som utövar offentlig makt alltid ska ha en behörighetsgrund som i sista hand återgår på en av riksdagen stiftad lag (RP 1/1998 rd, s. 76). För bestämmelser i lag gäller allmänna krav på exakthet och noggrannhet. Regleringen av befogenheter är enligt grundlagsutskottets uppfattning vanligen relevant också i förhållande till de i grundlagen inskrivna grundläggande fri- och rättigheterna (se GrUU 67/2016 rd, GrUU 10/2016 rd).

*Godtagbarhet och proportionalitet*

Vid militär underrättelseinhämtning bör de grundläggande fri- och rättigheterna och de mänskliga rättigheterna respekteras och proportionalitetsprincipen, principen om minsta olägenhet, principen om ändamålsbundenhet och förbudet mot diskriminering iakttas. Dessa rättigheter och principer ska styra all underrättelseverksamhet.

När en militärunderrättelsemyndighet ska välja vilken eller vilka av de metoder för underrättelseinhämtning som den inom ramen för sina befogenheter kan motivera, ska den metod väljas som bäst främjar tillgodoseendet av de grundläggande fri- och rättigheterna och de mänskliga rättigheterna.

Proportionalitetsprincipen förutsätter en bedömning av huruvida användningen av metoden är försvarbar i relation till hur viktigt och brådskande underrättelseuppdraget är och uppdragets huvudsakliga syfte och andra omständigheter som inverkar på den övergripande bedömningen av situationen. I sin avgörandepraxis har Europadomstolen och EU-domstolen understrukit proportionalitetsprincipens betydelse, särskilt i samband med underrättelseinhämtning som avser datatrafik (t.ex. Zakharov mot Ryssland, Weber och Saravia mot Tyskland, Digital Rights Ireland).

Därmed förutsätter underrättelseinhämtning som avser datatrafik att denna metod tas till i sista hand, dvs. att det är omöjligt eller oskäligt svårt att inhämta information med hjälp av någon annan metod. Iakttagandet av principen om minsta olägenhet innebär att militärunderrättelsemyndigheten inte får ingripa i någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenhet än vad som är nödvändigt för att utföra ett uppdrag. Militärunderrättelsemyndigheten får i enlighet med principen om ändamålsbundenhet använda befogenheten att inhämta underrättelser bara för ett lagfäst ändamål.

Inriktningen av åtgärderna inom den militära underrättelseinhämtningen ska göras på ett icke-diskriminerande sätt. En uttrycklig bestämmelse om detta har tagits in i lagförslag 1. Inriktningen av en åtgärd inom den militära underrättelseinhämtningen får inte enbart grunda sig på uppgifter om en persons ålder, ursprung, nationalitet, språk, religion, övertygelse, åsikt, politiska verksamhet, fackföreningsverksamhet, familjerelationer, hälsotillstånd, funktionsnedsättning eller sexuella inriktning.

Regleringen stärker likställighetsprincipen enligt 6 § 2 mom. i grundlagen inom underrättelseverksamheten. Den kan emellertid vara nödvändigt att avgränsa inriktningen av en åtgärd på grund av uppgifter om en person som avses ovan, t.ex. utifrån nationalitet. Detta förutsätter dock objektiva och tillräckliga grunder.

Grundlagens förbud mot diskriminering har inte ansetts förbjuda all åtskillnad mellan människor, även om åtskillnaden bygger på en av de särskilt nämnda grunderna i bestämmelsen om diskriminering. Det väsentliga är om det är möjligt att motivera åtskillnaden på ett sätt som är godtagbart med hänsyn till systemet för de grundläggande fri- och rättigheterna. Förslaget till bestämmelse är sålunda inte problematiskt med avseende 6 § 2 mom. i grundlagen.

*Rättsskyddsarrangemang*

Inom underrättelseverksamhet betonas rättsskyddsarrangemangen och tillsynens effektivitet och lämplighet. Också de skyldigheter som gäller de mänskliga rättigheterna och Europeiska unionens rättssystem förutsätter effektivitet och oberoende i övervakningen av användningen av befogenheter som gör intrång i skyddet för förtroliga meddelanden. Det är viktigt att militärunderrättelsemyndigheten inte har obegränsad prövningsrätt när det gäller inriktningen av informationsinhämtningen. Ett sätt att begränsa myndighetens prövningsrätt är att hänvisa beslut om användningen av sådana metoder för underrättelseinhämtning som innebär allvarligt intrång i de grundläggande fri- och rättigheterna till domstol (bl.a. Weber och Saravia mot Tyskland). Underrättelsemyndigheten ska inte kunna ha direkt och obegränsat tillträde till telekommunikationsnäten (Kennedy mot Förenade kungariket). Detta kan förebyggas genom att en koppling till telekommunikationsnätet i enlighet med ett domstolstillstånd för underrättelseinhämtning som avser datatrafik ska göras av någon annan instans än underrättelsemyndigheten.

Enligt Europadomstolen ska tillståndsprövningens område framgå av lag. Enligt förslaget ska yrkandets och beslutets innehåll regleras i lagen. En tillståndsprövning, som grundar sig på sökbegrepp eller på godkännande av en så exakt beskrivning som möjligt av den verksamhet eller de personer som äventyrar den nationella säkerheten kan anses uppfylla Europadomstolens krav. Det föreskrivs också i lagen vilka uppgifter som inte får utgöra sökbegrepp.

Sådana metoder för underrättelseinhämtning som enligt förslaget ska förutsätta tillstånd av domstol är teleavlyssning och inhämtande av uppgifter 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. Tillstånd får bevilja för högst sex månader åt gången, med undantag av metoderna teleavlyssning och inhämtande av information i stället för teleavlyssning i fråga om personer. Tillstånd får i sådana fall beviljas för högst tre månader åt gången.

När domstolen har beviljat tillstånd för underrättelseinhämtning som avser datatrafik, görs en koppling till den del av kommunikationsnätet som tillståndet gäller. Med den som utför en koppling och som upplåter datatrafiken enligt tillståndet avses en sådan tillhandahållare av nät- och infrastrukturtjänster som avses i 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät, dvs. aktiebolaget Suomen Erillisverkot Oy, eller ett dotterbolag som helt ägs av bolaget, dvs. Suomen Turvallisuusverkko Oy. Uppgiften har anvisats någon som är oberoende av underrättelsemyndigheterna för att på så sätt säkerställa att underrättelsemyndigheterna inte får mer omfattande tillgång till telekommunikationen än vad domstolens tillståndsbeslut medger. Förslaget till bestämmelser om förbud mot kopiering och underrättelse-

inhämtning och om underrättelse om användning av en metod för underrättelseinhämtning tryggar rättsskyddet. Rätten för en person att få kännedom om att han eller hon har blivit föremål för underrättelseinhämtning är viktigt för att det överhuvudtaget ska vara möjligt att söka rättsskydd. Den som blivit föremål för teleavlyssning, inhämtande av uppgifter i stället för teleavlyssning, teknisk observation eller underrättelseinhämtning som avser datatrafik ska utan dröjsmål meddelas om detta så snart syftet med användningen av metoden för underrättelseinhämtning har uppnåtts. Användningen av de övriga metoderna ska meddelas, om förundersökning har inletts i ärendet. Syftet med den föreslagna regleringen är att ge var och en som misstänker att han eller hon blivit föremål för en kränkning av skyddet för privatlivet möjlighet att få sin sak behandlad av domstol eller någon annan myndighet på behörigt sätt i enlighet med vad som förutsätts i 21 § i grundlagen.

Parters rätt till handling är en viktig garanti för rättsskyddet för den som blivit föremål för underrättelseinhämtning. All användning av underrättelseinhämtningsmetoder ska vara partsoffentliga så snart personen har underrättats om att en metod för underrättelseinhämtning har använts. I fråga om alla underrättelseinhämtningsmetoder gäller att diarier, handlingar, behandling och avgöranden är offentliga. Också partsoffentlighet gäller.

En effektiv tillsyn över underrättelseverksamheten förutsätter att tillsynsorganen har rätt att kontrollera uppgifter och handlingar. Därför omfattas metoderna för underrättelseinhämtning av skyldighet att utan dröjsmål föra protokoll.

Den externa laglighetsövervakningen av underrättelseverksamheten ska utöver av de högsta laglighetsövervakarna skötas av en ny myndighet, som ska övervaka underrättelseverksamheten i realtid (Klass m.fl. mot Tyskland). För att en övervakning i realtid ska var möjlig, föreskrivs det om skyldigheten att ge underrättelseombudsmannen information om domstolens beslut och tillstånd som gäller underrättelseinhämtningsmetoder så snart som möjligt efter domstolens beslut. Dessutom ska militärunderrättelsemyndigheten så snart som möjligt meddela underrättelseombudsmannen om beslut som gäller andra underrättelseinhämtningsmetoder än sådana som omfattas av domstolens beslutsbehörighet och om skyddande av underrättelseinhämtning, yppandeförbud och överföring av en uppgift som ska lämnas ut för brottsbekämpningen (104 § i lagförslag 1).

Ombudsmannen har omfattande rätt att få information och rätt att få utredningar av myndigheter och andra som handhar offentliga förvaltningsuppgifter. Ombudsmannen kan utföra inspektioner för att kontrollera lagligheten i underrättelseverksamheten, och det föreslås dessutom att ombudsmannen ska ha rätt att få sådan tillgång till utrymmen och informationssystem som är nödvändig för tillsynen. Dessutom ska en underrättelseinhämtningsmetod kunna avbrytas eller avslutas, om ombudsmannen anser att tillsynsobjektet förfar lagstridigt i sin underrättelseinhämtning.

Bestämmelser om övervakningen av lagenligheten i den militära underrättelseinhämtningen inom försvarsförvaltningen ingår i 10 kap. i lagförslag 1. Övervakningen av lagenligheten i den militära underrättelseinhämtningen inom försvarsförvaltningen ska effektiveras jämfört med nuläget med hjälp av ytterligare personella resurser. Underrättelseverksamheten inom Försvarsmakten ska övervakas av chefen för Huvudstaben och Försvarsmaktens assessor.

Den tjänsteman som leder användningen av en metod för underrättelseinhämtning och en tjänsteman som använder en sådan metod eller en av denne förordnad tjänsteman ska utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av metoden för underrättelseinhämtning. Granskningen av upptagningar och handlingar har en

väsentlig betydelse för att den tjänsteman som ansvarar för verksamheten eller den tjänsteman som förordnats för uppgiften de facto i realtid ska kunna övervaka att metoderna för underrättelseinhämtning används lagenligt.

Försvarsministeriet föreslås ha rätt att granska de beslut som fattats, upptagningar som uppkommit och handlingar som upprättats samt annat material som uppkommit inom den militära underrättelseinhämtningen. Trots sekretessbestämmelserna har försvarsministeriet rätt att få uppgifter om omständigheter som anknyter till den militära underrättelseinhämtningen och som är av betydelse samhälleligt, ekonomiskt eller till sin allvarlighetsgrad. Försvarsministeriet ska årligen till riksdagens justitieombudsman och till underrättelseombudsmannen ge en berättelse om hur metoderna för underrättelseinhämtning och skyddandet av den militära underrättelseinhämtningen har använts och övervakats.

Europadomstolen har ansett det vara viktigt att folkrepresentationens företrädare deltar i övervakningen av underrättelseverksamheten som en garant för att regeringen handlar ansvarsfullt. Riksdagen svarar också för godkännandet av underrättelsemyndigheternas budget. Det föreslås att den parlamentariska övervakningen av underrättelseverksamheten anförtros ett utskott för övervakning av underrättelseverksamheten. Utskottet ska ingå i riksdagens utskottsväsende. För att kunna sköta sin tillsynsuppgift ska utskottet utöver rätten till information också ha rätt att få utredningar av bl.a. underrättelseombudsmannen och andra myndigheter.

### 4.3 De övriga lagförslagens förhållande till grundlagen

*Yttrandefrihet och rättssäkerhet*

I 92 § i lagförslag 1 i propositionen föreslås bestämmelser om yppandeförbud, som gäller metoder för underrättelseinhämtning. En utomstående som har bistått vid utförandet av ett underrättelseuppdrag får inte röja uppgifter eller omständigheter som kommit till dennes kännedom om underrättelseuppdraget.

Grundlagens 12 § 1 mom. innehåller en generalklausul om yttrandefrihet, en bestämmelse om de rättigheter som räknas till yttrandefriheten, ett förbud mot att i förväg uppställa hinder för utövandet av dessa rättigheter, ett lagförbehåll, dvs ett krav på att bestämmelser om reglering av yttrandefriheten ska utfärdas genom lag och ett kvalificerat lagförbehåll om begränsningar som är nödvändiga för att skydda barn i fråga om bildprogram.

Det centrala syftet med yttrandefrihetsbestämmelsen är att garantera fri opinionsbildning, öppen offentlig debatt, fri utveckling och pluralism gällande massmedierna samt möjlighet till offentlig kritik av maktutövningen, vilka utgör förutsättningar för ett demokratiskt samhälle. Förslagen till bestämmelser om yppandeförbud gällande enskilda personer och ärenden har bedömts med tanke på yttrandefriheten (GrUU 28/2008 rd, GrUU 67/2002 rd, GrUU 28/1997 rd).

Yppandeförbudet kan inte anses begränsa den i 12 § 1 mom. i grundlagen tryggade yttrandefriheten med beaktande av de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna, särskilt kravet på exakthet och noggrann avgränsning samt kravet på godtagbarhet. I lagen föreslås detaljerade bestämmelser om de villkor som ställs för meddelande av yppandeförbud.

Yppandeförbudet bör betraktas som nödvändigt, eftersom det att en person som är föremål för informationsinhämtning får kännedom om användningen av en metod för underrättelsein-

hämtning genom en utomstående kan förhindra användning av metoden eller äventyra att syftet med metoden uppnås. Eftersom överträdelse av yppandeförbudet ska bestraffas som sekretessbrott eller sekretessförseelse med stöd av 38 kap. 1 eller 2 § i strafflagen, kopplas den föreslagna bestämmelsen dessutom ihop med straffrättslig begränsning av yttrandefriheten, dvs. ett s.k. yttrandefrihetsbrott.

Ett beslut om yppandeförbud får inte överklagas genom besvär. I beslutet ska nämnas besvärsförbudet och den rättsliga grunden för förbudet. Den som omfattas av ett yppandeförbud får alltid meddela underrättelseombudsmannen om yppandeförbudet. Militärunderrättelsemyndigheterna ska vidare med stöd av 105 § i lagförslag 1 göra en anmälan om yppandeförbudet till underrättelseombudmannen. Eftersom en militärunderrättelsemyndighet i praktiken aldrig har behov, eller ens rätt, att offentligt informera om sådana omständigheter som gäller användning av metoder för underrättelseinhämtning och som omfattas av yppandeförbudet, är meddelandet av yppandeförbud inte förknippat med en liknande diskrepans som kan framkomma vid förundersökning när förundersökningsledaren informerar om de omständigheter i fråga om vilka den misstänkte eller dennes medhjälpare har meddelats yppandeförbud.

Besvärsförbudet kränker inte den i 21 § 2 mom. i grundlagen tryggade rätten att söka ändring med beaktande av de vägande skäl som förutsätts för att förbud ska meddelas och det faktum att förbudet riktas mot omständigheter som gäller användningen av metoder för underrättelseinhämtning. Vidare ska den som har fått ett yppandeförbud informeras om möjligheten att anföra klagan hos hovrätten och om möjligheten att meddela underrättelseombudsmannen om yppandeförbudet. Rätten att anföra klagomål och underrättelseombudsmannens övervakning kan tillsammans betraktas som en tillräcklig garanti för rättsskydd (Klass m.fl. mot Tyskland och Leander mot Sverige).

Enligt 98 § i lagförslaget om militär underrättelseverksamhet får omprövning av ett beslut om ersättning till ett teleföretag eller en dataöverförare begäras på det sätt som anges i förvaltningslagen. Ett beslut som meddelats med anledning av en begäran om omprövning får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen. Över förvaltningsdomstolens beslut får besvär dessutom anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd. Bestämmelserna är inte problematiska med avseende på rättsskyddet enligt 21 § 1 mom. i grundlagen.

I 110 § i lagförslaget om militär underrättelseverksamhet föreslås bestämmelser om tystnadsplikt för tjänstemän som är anställda vid militärunderrättelsemyndigheterna och för den som utför ett underrättelseuppdrag under ledning och övervakning av militärunderrättelsemyndigheterna. Förslaget har stor betydelse med avseende på yttrandefriheten enligt 12 § i grundlagen.

De som berörs av tystnadsplikt motsvarar delvis i fråga om innehållet de bestämmelser i 24 § 1 mom. 7, 9 och 10 punkten i lagen om offentlighet i myndigheternas verksamhet som har reglerats med grundlagsutskottets medverkan (GrUU 43/1998 rd). Förslaget till bestämmelse är således inte problematiskt med avseende på offentlighetsprincipen enligt 12 § 2 mom. i grundlagen.

*Egendomsskydd*

I 93 § i lagförslag 1 föreslås bestämmelser om teleföretags biståndsskyldighet och i 94 och 95 § föreslås bestämmelser om dataöverförarens biståndsskyldighet.

De skyldigheter som åläggs teleföretag och dataöverförare ska anses vara oproblematiska med avseende på det egendomsskydd som tryggas i 15 § 1 mom. i grundlagen, eftersom skyldigheterna grundar sig på exakta bestämmelser och de är skäliga med avseende på de företag som saken gäller (GrUU 8/2002 rd och 61/2002 rd). Med avseende på skälighetsbedömningen bör hänsyn tas till att dataöverföraren inte har ålagts skyldighet att lämna militärunderrättelsemyndigheterna sådana uppgifter som saknar betydelse för inriktandet och att dataöverförarens skyldighet att lämna uppgifter endast gäller sådana uppgifter som denne redan har i sin besittning. Det föreslås att de kostnader som biståndsskyldigheten orsakar teleföretag och de kostnader som skyldigheten att lämna uppgifter orsakar dataöverföraren ska ersättas.

Trots att en sammanslutnings medlemmar, revisorer, verkställande direktör, styrelsemedlemmar eller arbetstagare är bundna av företags-, bank- eller försäkringshemlighet har militärunderrättelsemyndigheterna med stöd av 101 § i lagförslaget om militär underrättelseverksamhet på begäran rätt att få sådana uppgifter som i ett enskilt fall kan antas vara behövliga vid utredningen av sådan verksamhet som avses i 4 §.

Bestämmelsen har betydelse för den som är föremål för begäran om information för att denne inte vid lämnande av information ska göra sig skyldig till sekretessbrott eller något annat straffbart brott, utan kan lita på att han eller hon har agerat som lagen tillåter. Den bestämmelse som gäller rätten att få information av privata sammanslutningar är oproblematisk inte bara med avseende på det skydd för privatlivet som tryggas i 10 § 1 mom. i grundlagen utan även med avseende på det egendomsskydd som tryggas i 15 § 1 mom. i grundlagen, med beaktande av det nödvändiga samhälleliga behov som ligger bakom den föreslagna paragrafen, förutsägbarheten i fråga om den yppandeskyldighet som anges i lagen med avseende på de parter som berörs samt det faktum att de förväntningar på resultat som hänför sig till begäran kopplas till exakta kriterier.

I 62 § i lagförslaget om militär underrättelseverksamhet finns bestämmelser om militär underrättelseinhämtning utomlands. Beslut om militär underrättelseinhämtning och användning av metoder för underrättelseinhämtning som sker utanför Finland ska fattas av Huvudstabens underrättelsechef.

Det är klart att en finländsk tjänsteman inte heller utomlands kan verka i strid med universella grundläggande och mänskliga rättigheter. På grund av detta och med beaktande av att informationen om att någon har blivit föremål för användning av metoder för underrättelseinhämtning är en viktig garanti för rättsskyddet, ska användning av metoder för underrättelseinhämtning i princip underrättas även vid verksamhet utomlands. Detta är emellertid inte alltid möjligt. I vissa situationer kan underrättelse av detta slag inte bara skada Finlands internationella förbindelser eller förutsättningar för internationellt samarbete, utan även äventyra liv och hälsa hos den tjänsteman som utför militär underrättelseinhämtning. Underrättelse om användning av en metod för underrättelseinhämtning kan vara omöjlig i t.ex. sådana länder som i fråga om sin förvaltning har kollapsat eller är bräckliga och där det inte finns myndighetsregister eller andra medel att utreda identitet eller boningsort för den som är föremål för inhämtandet av information. På grund av detta och med beaktande av att underrättelse om användning av en metod för underrättelseinhämtning med stöd av 86 § 2 mom. kan förbises helt och hållet även i Finland, kan de föreslagna bestämmelserna vad gäller det prövning underkastade underrättelsearrangemanget inte anses vara problematiska med avseende på rättsskyddet enligt 21 § i grundlagen.

*Överföring av förvaltningsuppgifter på andra än myndigheter*

De förslag till bestämmelser som gäller internationellt samarbete, genomförande av den koppling som underrättelseinhämtning som avser datatrafik förutsätter och deltagande i militär underrättelseverksamhet för en reservist som tjänstgör i enlighet med värnpliktslagen ska bedömas i ljuset av grundlagens bestämmelser om överföring av förvaltningsuppgifter på andra än myndigheter.

Enligt 124 § i grundlagen kan offentliga förvaltningsuppgifter anförtros andra än myndigheter endast genom lag eller med stöd av lag om det behövs för en ändamålsenlig skötsel av uppgifterna och det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning. Uppgifter som innebär betydande utövning av offentlig makt får dock ges endast myndigheter (RP 1/1998 rd, s. 62).

Enligt förarbetena till grundlagen och grundlagsutskottets praxis ska t.ex. på självständig prövning baserad rätt att använda maktmedel eller att på något annat konkret sätt ingripa i en enskild persons grundläggande fri- och rättigheter betraktas som betydande utövning av offentlig makt.

I 19 § i lagen om militär underrättelseverksamhet föreslås bestämmelser om internationellt samarbete. Militärunderrättelsemyndigheterna ska kunna samarbeta och utbyta underrättelseuppgifter med utländska underrättelse- och säkerhetstjänster. Bestämmelser om beslutsfattandet om lämnande av och begäran om internationellt bistånd finns i lagen om beslutsfattande om lämnande av och begäran om internationellt bistånd (418/2017).

En förutsättning för att en tjänsteman från en främmande stat ska kunna verka i Finland är ett uttryckligt beslut av Huvudstabens underrättelsechef. Tjänstemannens verksamhet i Finland ska vara av tillfällig karaktär och alltid ske under uppsikt och övervakning av en finländsk tjänsteman. En främmande stats tjänsteman omfattas när han eller hon utövar tjänsteuppdrag i Finland av straff- och skadeståndsrättsligt ansvar, om inte annat föranleds till exempel av tjänstemannens diplomatstatus. I en situation där en främmande stats tjänsteman i Finland använder vissa i paragrafen specificerade metoder för underrättelseinhämtning är det således inte fråga om en uppgift som innebär betydande utövning av offentlig makt som endast får ges myndigheter enligt 124 § i grundlagen. Av dessa orsaker bedöms de föreslagna bestämmelserna inte äventyra de krav på garanterandet av de grundläggande rättigheterna och rättsskyddet samt en god förvaltning som ställs på utövning av offentlig makt.

Uppgiften att styra datatrafiken enligt tillståndet till militärunderrättelsemyndigheten för den som utför kopplingen är till sin karaktär inte utövning av offentlig makt som förutsätter utövande av oberoende prövningsrätt utan verkställande i enlighet med ett tillstånd som en domstol har beviljat. Trovärdigheten och tillförlitligheten för underrättelseinhämtning som avser datatrafik ökas av att militärunderrättelsemyndigheterna inte har tillträde till annan datatrafik än den som tillstånden gäller.

Det har inte fastställts några principiella begränsningar för att använda beväringar och andra värnpliktiga som tjänstgör i sådan tjänstgöring som grundar sig på den skyldighet att försvara landet som fastställs i 127 § i grundlagen. Vid reservens repetitionsövningar upprätthålls den militära kunskap och förmåga som inhämtats under beväringstjänsten samt ges utbildning för mera krävande uppgifter. När reservister biträder en militärunderrättelsemyndighet har de med stöd av 88 § rätt att utöva befogenheter endast under uppsikt och övervakning av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman. Det ska föreskrivas uttryckligen om de metoder för underrättelseinhämtning som de får använda och de ska inte få inhämta information om innehållet i ett meddelande. Reservisterna ska ha kun-

skaps- och färdighetsmässiga förutsättningar att utföra uppgifterna. Motsvarande bestämmelser om reservisters befogenheter finns i 10 kap. i lagen om militär disciplin och brottsbekämpning inom försvarsmakten, som gäller allvarliga störningar under normalförhållanden samt undantagsförhållanden. Det är således inte fråga om utövande av oberoende prövningsrätt eller betydande utövning av offentlig makt.

*Ansvar för ämbetsåtgärder*

I 112 § i lagen om militär underrättelseverksamhet föreslås en bestämmelse enligt vilken en tjänsteman vid en militärunderrättelsemyndighet vid utförandet av ett tjänsteuppdrag ska presentera sig som tjänsteman vid en militärunderrättelsemyndighet eller på begäran visa upp sitt tjänstetecken. Militärunderrättelsemyndigheterna ska se till att en tjänsteman som har utfört ett tjänsteuppdrag vid behov kan identifieras. Kravet på att tjänstemannen ska kunna identifieras baserar sig på 118 § i grundlagen, enligt vilken en tjänsteman svarar för att hans eller hennes ämbetsåtgärder är lagliga.

Enligt 118 § 3 mom. i grundlagen har var och en som har lidit rättskränkning eller skada till följd av en lagstridig åtgärd eller försummelse av en tjänsteman eller någon som sköter ett offentligt uppdrag rätt att yrka att denne döms till straff samt kräva skadestånd. För att denna rätt enligt 118 § 3 mom. i grundlagen ska kunna förverkligas i praktiken, måste en tjänsteman som utför ett tjänsteuppdrag vid behov kunna identifieras.

### 4.4 Bedömning av propositionen med avseende på Europadomstolens avgörandepraxis

Utifrån Europadomstolens avgörandepraxis och grundlagsutskottets tolkningspraxis, för vilka det har redogjorts i allmänna motiveringen, utvärderas det nedan hur de föreslagna bestämmelserna uppfyller kriterier som är tillräckliga för att de grundläggande och mänskliga rättigheterna ska tillgodoses.

I 5-8 § i lagförslaget om militär underrättelseverksamhet föreslås bestämmelser om de allmänna principer som ska iakttas i myndigheterna verksamhet och som begränsar möjligheterna till godtycke (Malone mot Förenade kungariket, Amann mot Schweiz, Telegraaf Media Nederland Landelijke Media B.V. m.fl. mot Nederländerna, Rotaru mot Rumänien). Principerna styr myndigheterna att använda sina befogenheter i rätt proportion så att individen orsakas så få olägenheter som möjligt, så att befogenheterna används endast för föreskrivet ändamål och så att användning av befogenheten inte kan grunda sig på ett diskriminerande inriktande.

I lagförslagets 4 § föreskrivs om föremålen för den militära underrättelseinhämtningen. Föremålen för den militära underrättelseinhämtningen har beskrivits så noggrant avgränsat och exakt som möjligt (bl.a. Klass mot Tyskland, Weber och Saravia mot Tyskland, Kopp mot Tyskland, Kruslin mot Frankrike och Huvig mot Frankrike). Förteckningen över föremålen för den militära underrättelseinhämtningen är uttömmande och det bedöms att den uppfyller de krav som Europadomstolen ställer i sin avgörandepraxis. Bestämmelser om föremålen för den militära underrättelseinhämtningen begränsar myndigheternas möjligheter att använda metoder för underrättelseinhämtning samt ett slumpmässigt inriktande av metoderna mot vem som helst (Amann mot Schweiz).

Utöver de föremål för den militära underrättelseinhämtningen som anges i lagen finns i 3 § bestämmelser om syftet med den militära underrättelseinhämtningen, dvs. för vilka ändamål

den information som inhämtats vid militär underrättelseinhämtning ska användas (Liberty m.fl. mot Förenade kungariket).

Bestämmelserna i 3 och 4 § i lagförslaget kan tillsammans bedömas tillgodose det krav som Europadomstolen ställer på att ett ingripande i de rättigheter som garanteras i artikel 8 i Europakonventionen är nödvändigt i ett demokratiskt samhälle och att den nationella säkerheten skyddas genom lag (bl.a. Weber och Saravia mot Tyskland, Kennedy mot Förenade kungariket). Av detta följer att klargörandet av begreppet nationell säkerhet i första hand måste överlåtas åt nationell praxis (Kennedy mot Förenade kungariket). Dessutom hör bedömningen av om ett ingripande är nödvändigt i första hand till den nationella lagstiftarens uppgifter (Silver m.fl. mot Förenade kungariket, Handyside mot Förenade kungariket).

En uttömmande förteckning över föremålen för den militära underrättelseinhämtningen kan anses tillgodose förutsättningen i Europadomstolens avgörandepraxis om att en lag som ingriper i skyddet för privatlivet och som möjliggör en hemlig myndighetsåtgärd till sin art ska vara sådan att medborgarna kan förutse vilka följder tillämpningen av den får för dem själva (bl.a. Kruslin mot Frankrike, Huvig mot Frankrike, Lambert mot Frankrike). Vidare bedöms lagförslaget vara tillräckligt tydligt så att det visar under vilka förhållanden och under vilka förutsättningar medborgarna kan bli föremål för hemliga myndighetsåtgärder. För att intrång ska kunna göras i en persons privatliv med stöd av denna proposition ska personen i fråga ha en beröringspunkt med den verksamhet som avses i lagens 4 §, och utöver detta ska man med en metod för underrättelseinhämtning med fog kunna anta att man får information med avseende på ett underrättelseuppdrag (11 §). Om det är fråga om att en person deltar i annan än militär verksamhet, är förutsättningen för att sådana befogenheter som gör intrång i skyddet för förtroliga meddelanden får användas att personen i fråga deltar i verksamhet som allvarligt hotar den nationella säkerheten. Användning av befogenheten begränsas dessutom i fråga om olika befogenheter av särskilda användningsändamål, t.ex. att användningen av en metod för underrättelseinhämtning kan antas vara av synnerlig vikt eller att den är nödvändig för att få information med avseende på ett underrättelseuppdrag.

Tillgodoseendet av kravet på förutsebarhet stöds även av det att användningen av befogenheterna är tidsmässigt begränsad, högst tre eller sex månader, och i fråga om den inhämtade informationen gäller skyldighet att granska informationen (107 §) och skyldighet att utplåna information (81-82 och 84 §) samt förbud mot underrättelseinhämtning (79-80 §) (Weber och Saravia mot Tyskland). När det gäller att förvara informationen bör bestämmelserna i lagen om offentlighet i myndigheternas verksamhet beaktas.

Metoderna för underrättelseinhämtning motsvarar radiosignalspaning, underrättelseinhämtning som avser utländska datasystem och underrättelseinhämtning som avser datatrafik med undantag för de befogenheter för hemligt inhämtande av information som anges i 5 kap. i polislagen. Om de hemliga metoderna för inhämtande av information har föreskrivits med grundlagsutskottets medverkan (GrUU 67/2010 rd). Vidare får metoder för underrättelseinhämtning inte användas för att få information från ett utrymme som används för stadigvarande boende. De aktuella befogenheterna kan således bedömas uppfylla de förutsättningar som grundlagsutskottet uppställt för befogenheterna.

Den underrättelseinhämtning som avser datatrafik kan bedömas uppfylla kraven i Europadomstolens avgörandepraxis. Användning av underrättelseinhämtning som avser datatrafik och som riktar sig mot någon annan än en statlig aktör ska vara möjlig när den riktar sig mot i 4 § avsedd verksamhet, och enligt 11 § i lagförslag 1 kan det med fog antas att man får information med avseende på ett underrättelseuppdrag (Liberty och övriga mot Förenade kungariket).

Användningen av underrättelseinhämtning som avser datatrafik ska dessutom enligt 67 § i lagförslag 1 vara nödvändig (Szabó och Vissy mot Ungern) för att inhämta information med avseende på ett underrättelseuppdrag. Underrättelseinhämtning som avser datatrafik förutsätter på grund av 68 § i lagförslag 1 tillstånd av domstol (Weber och Saravia mot Tyskland). I ett tillståndsyrkande ska vidare anges de sökbegrepp som används vid underrättelseinhämtning som avser datatrafik eller kategorier av sökbegrepp samt motivering för dessa (Liberty och övriga mot Förenade kungariket). En underrättelsemyndighet ska inte ha direkt tillträde till kommunikationsnäten, utan en utomstående part utför kopplingen i enlighet med domstolens tillstånd.

Underrättelseinhämtning som avser datatrafik ska vara 1) fysiskt avgränsad, 2) underrättelseinhämtningen sker i enlighet med underrättelsemyndigheternas sökbegrepp som en utomstående part har bedömt, 3) informationsinhämtningen är tidsmässigt begränsad och 4) endast en liten del av den information som rör sig i datakommunikationsnäten sparas för underrättelsemyndigheten.

Enligt Europadomstolens avgörandepraxis är underrättelsemyndigheterna skyldiga att underrätta om användning av en metod för underrättelseinhämtning (bl.a. Zakharov mot Ryssland, Klass m.fl. mot Tyskland, Weber och Saravia mot Tyskland), vilket bestämmelsen i 86 § i lagförslag 1 tillgodoser. Enligt 86 § i lagförslag 1 fattar domstolen beslut om att underrättelsen får utebli (särskilt Klass m.fl. mot Tyskland, Weber och Saravia mot Tyskland).

Tillgodoseendet av rättsskyddet kompletteras förutom av underrättelseskyldigheten dessutom av utomstående oberoende rättslig övervakning (bl.a. Klass m.fl. mot Tyskland, Leander mot Sverige). Utifrån en underrättelse kan en individ meddela underrättelseombudsmannen om åtgärder som behöver vidtas.

Ett nytt utomstående och oberoende organ, underrättelseombudsmannen, inrättas för att övervaka underrättelseverksamheten. Övervakningens effektivitet och tillsynsorganens oberoende är viktiga krav med tanke på underrättelseverksamhetens godtagbarhet (Liberty m.fl. mot Förenade kungariket). Underrättelseombudsmannen ska ha en omfattande rätt att få information och rätt att avbryta verksamheten. Den övervakning som utförs av underrättelseombudsmannen kan anses uppfylla kraven i Europadomstolens avgörandepraxis (Szabó och Vissy mot Ungern, Dumitru Popescu mot Rumänien). Dessutom ska folkrepresentationen för sin del delta i övervakningen av underrättelseverksamheten, via ett utskott som inrättas vid riksdagen (Campbell mot Förenade kungariket, Leander mot Sverige), vilket Europadomstolen har fäst vikt vid.

Propositionen kan bedömas uppfylla kraven i Europadomstolens avgörandepraxis och grundlagsutskottets tolkningspraxis om att det ska föreskrivas om begränsningarna i lag, att lagen ska grunda sig på skyddet för den nationella säkerheten och att ingripandet ska vara nödvändigt i ett demokratiskt samhälle. I lagen definieras i enlighet med Europadomstolens krav på förutsebarhet arten och omfattningen av de observationsbefogenheter som ska utövas i hemlighet (20–75 §), de personkategorier som befogenheterna får utövas mot (11 §), arten av den verksamhet som ger anledning till att utöva befogenheterna (4 §), de förfaranden som ska följas när den information som inhämtas med hjälp av befogenheterna undersöks, utnyttjas, sparas, distribueras vidare och undanröjs (79–86 § samt i fråga om personuppgifter i lagen om behandling av personuppgifter inom försvarsmakten), samt övervakningen av befogenheterna (102–105 § samt lagen om övervakning av underrättelseverksamheten) och rättsmedel som gäller dessa (86 § och lagen om övervakning av underrättelseverksamheten).

### 4.5 Bedömning av lagstiftningsordningen

De lagförslag som ingår i propositionen kan enligt regeringens uppfattning behandlas i vanlig lagstiftningsordning, med undantag för sådana förslag till bestämmelser om behörighet, som innebär ingrepp i den hemlighet i fråga om förtroliga meddelanden som tryggas i 10 § 2 mom. i grundlagen.

Sådana förslag till bestämmelser i lagförslag 1 är 24 § (teknisk avlyssning), 30 § (teknisk observation av utrustning), 32 § 3 mom. (teleavlyssning av någon annan än en statlig aktör), 33 § (inhämtande av information i stället för teleavlyssning av någon annan än en statlig aktör), 35 § 3 mom. (teleövervakning av någon annan än en statlig aktör), 55 § (kopiering av någon annans än en statlig aktörs meddelande) och 67 § (underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer).

Med stöd av den nya begränsningsgrund som gäller inhämtande av information som föreslås till 10 § 4 mom. i grundlagen ska det dock vara möjligt att lagstifta om dem i vanlig lagstiftningsordning.

Ovan uppräknade befogenheter har samband med den föreslagna ändringen av grundlagen. Av denna anledning och också på grund av de övriga statsförfattningsrättsliga aspekterna i anslutning till propositionen anser regeringen det vara ändamålsenligt att riksdagen inhämtar grundlagsutskottets utlåtande om propositionen. Alla regeringens propositioner som gäller underrättelseverksamheten är beroende av varandra och bör därför enligt regeringens åsikt föras till grundlagsutskottet för behandling tillsammans.

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

*Lagförslag*

**1.**

# Lag

## om militär underrättelseverksamhet

I enlighet med riksdagens beslut föreskrivs

1 kap.

### Allmänna bestämmelser

1 §

*Tillämpningsområde*

Denna lag innehåller bestämmelser om syftet med Försvarsmaktens underrättelseverksamhet (militär underrättelseinhämtning), om myndigheternas uppgifter och befogenheter, om beslutsfattande samt om styrningen av den militära underrättelseinhämtningen och övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen. Lagen innehåller också bestämmelser om det tekniska genomförandet av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning.

2 §

*Förhållande till annan lagstiftning*

Bestämmelser om civil underrättelseinhämtning finns i 5 a kap. i polislagen (872/2011) och i lagen om civil underrättelseinhämtning avseende datatrafik ( / ).

Bestämmelser om Försvarsmaktens brottsbekämpning finns i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014).

Bestämmelser om övervakning av underrättelseverksamheten finns i lagen om övervakning av underrättelseverksamheten ( / ). Bestämmelser om behandling av personuppgifter finns i lagen om behandling av personuppgifter inom Försvarsmakten ( / ).

3 §

*Syftet med den militära underrättelseinhämtningen*

Syftet med den militära underrättelseinhämtningen är att inhämta och behandla information om yttre hot för att Försvarsmakten ska kunna utföra sina uppgifter enligt 2 § 1 mom. 1 punkten underpunkterna a och b samt 3 och 4 punkten i lagen om försvarsmakten (551/2007) och stödja den högsta statsledningens beslutsfattande.

4 §

*Föremål för den militära underrättelseinhämtningen*

Med en metod för underrättelseinhämtning får information inhämtas om följande verksamhet, om verksamheten till sin art är militär:

1) verksamhet som bedrivs av en främmande stats väpnade styrkor och av med dem jämförbara organiserade trupper samt förberedelse för sådan verksamhet,
2) underrättelseverksamhet som riktar sig mot Finlands försvar,
3) planering, tillverkning, spridning och användning av massförstörelsevapen,
4) en främmande stats utvecklande och spridning av militärmateriel,
5) en kris som hotar internationell fred och säkerhet,
6) verksamhet som hotar säkerheten vid internationella krishanteringsinsatser,
7) verksamhet som hotar säkerheten i samband med att Finland ger internationellt bistånd och i samband med annan internationell verksamhet.

Vidare får det med en metod för underrättelseinhämtning inhämtas information om en främmande stats verksamhet eller någon annan sådan verksamhet som kan äventyra det finska försvaret eller som äventyrar samhällets vitala funktioner.

5 §

*Proportionalitetsprincipen*

Den militära underrättelseinhämtningens åtgärder ska vara försvarbara i förhållande till hur viktiga och nödvändiga de uppgifter är som erhålls genom informationsinhämtningen och till hur brådskande det är att erhålla uppgifterna, till det eftersträvade målet för den militära underrättelseinhämtningen, till föremålet för den militära underrättelseinhämtningen, till den kränkning av rättigheter som andra orsakas av att en underrättelseåtgärd används samt till andra omständigheter som påverkar saken.

6 §

*Principen om minsta olägenhet*

Genom användning av den militära underrättelseinhämtningens befogenheter får det inte ingripas i någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenhet än vad som är nödvändigt för utförande av uppdraget.

7 §

*Principen om ändamålsbundenhet*

Den militära underrättelseinhämtningens befogenheter får endast användas för de syften som anges i denna lag.

8 §

*Förbud mot diskriminering*

Inriktningen av åtgärderna inom den militära underrättelseinhämtningen ska göras på ett icke-diskriminerande sätt. Inriktningen av en åtgärd inom den militära underrättelseinhämt-

ningen får inte enbart grunda sig på uppgifter om en persons ålder, ursprung, nationalitet, språk, religion, övertygelse, åsikt, politiska verksamhet, fackföreningsverksamhet, familjeförhållanden, hälsotillstånd, funktionsnedsättning eller sexuella läggning.

9 §

*Definitioner*

I denna lag avses med

1) *den som utför en koppling* en sådan tillhandahållare av nät- och infrastrukturtjänster som avses i 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) eller ett dotterbolag som helt ägs av tillhandahållaren,

2) *lokaliseringsuppgift* en i 3 § 18 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) avsedd lokaliseringsuppgift,

3) *teleföretag* ett i 3 § 27 punkten i lagen om tjänster inom elektronisk kommunikation avsett teleföretag,

4) *dataöverförare* den som äger eller innehar en del av ett kommunikationsnät som överskrider Finlands gräns,

5) *metod för underrättelseinhämtning* de befogenheter som militärunderrättelsemyndigheterna har enligt 4 kap.,

6) *underrättelseuppdrag* ett uppdrag som Huvudstabens underrättelsechef ger en militärunderrättelsemyndighet för att inhämta underrättelseinformation om ett i 4 § avsett föremål för militär underrättelseinhämtning, vilket grundar sig på de prioriteringar som det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president förberedelsevis har behandlat eller på en begäran om information enligt 13 §,

7) *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 för utförande av ett underrättelseuppdrag,

8) *datatrafikens tekniska data* andra uppgifter om datatrafiken än de som hör till innehållet i ett meddelande,

9) *identifieringsuppgifter* 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,

10) *statlig aktör* en identifierad myndighet i en främmande stat eller en med en sådan jämställbar aktör samt den som är i dennes tjänst eller lyder under och styrs av denne,

11) *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,

12) *sammanslutningsabonnent* en i 3 § 41 punkten i lagen om tjänster inom elektronisk kommunikation avsedd sammanslutningsabonnent.

10 §

*Militärunderrättelsemyndigheter*

Militärunderrättelsemyndigheter är Huvudstaben och Försvarsmaktens underrättelsetjänst, vilka kan inhämta information för utförande av ett underrättelseuppdrag på det sätt som föreskrivs i denna lag.

Bestämmelser om militär underrättelseverksamhet i försvarsgrenarna finns i 58 §. Försvarsgrenarna är underställda militärunderrättelsemyndigheterna i den militära underrättelseverksamheten.

11 §

*Allmänna förutsättningar för användning av metoder för underrättelseinhämtning*

En allmän förutsättning för användning av en metod för underrättelseinhämtning är att det med fog kan antas att man genom metoden kan få information med avseende på ett underrättelseuppdrag.

Om föremålet för användningen av en metod för underrättelseinhämtning är någon annan än en statlig aktör, får teknisk avlyssning, teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, kopiering som riktas mot ett meddelande, sådan kopiering av en försändelse som riktas mot ett meddelande, underrättelseinhämtning som avser utländska datasystem och underrättelseinhämtning som avser datatrafik användas för underrättelseinhämtning i fråga om sådan verksamhet som avses i 4 § 2 mom., endast om verksamheten allvarligt hotar den nationella säkerheten.

Metoderna för underrättelseinhämtning enligt denna lag får användas i hemlighet för dem som är föremål för metoderna.

Användningen av en metod för underrättelseinhämtning ska avslutas före utgången av den tid som anges i beslutet eller tillståndet så snart syftet med användningen har nåtts eller det inte längre finns förutsättningar för användning av metoden.

2 kap.

**Styrning av och tillsyn över den militära underrättelseinhämtningen**

12 §

*Styrning och ledning av den militära underrättelseinhämtningen*

Det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president behandlar förberedelsevis prioriteringarna för föremålen för den militära underrättelseinhämtningen.

Försvarsministeriet styr den militära underrättelseinhämtningen administrativt och underrättar Försvarsmakten om de förberedelsevis behandlade prioriteringarna som avses i 1 mom.

Huvudstaben leder den militära underrättelseverksamheten med iakttagande av prioriteringarna för den militära underrättelseinhämtningen.

13 §

*Begäran om information*

Republikens president, statsrådets kansli, utrikesministeriet och försvarsministeriet kan av Huvudstaben begära information om föremålen för den militära underrättelseinhämtningen i överensstämmelse med de prioriteringar som avses i 12 § 1 mom.

14 §

*Samordning av underrättelseverksamheten*

Den militära och den civila underrättelseverksamheten samordnas mellan republikens president, statsrådets kansli, utrikesministeriet, försvarsministeriet och inrikesministeriet samt vid behov mellan andra ministerier och myndigheter.

Om det bedöms att den militära underrättelseverksamheten har utrikes- och säkerhetspolitiska konsekvenser, ska ärendet förberedelsevis behandlas mellan de myndigheter som avses i 1 mom.

15 §

*Tillsynen över den militära underrättelseinhämtningen*

Försvarsministeriet ger det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president en redogörelse för de prioriteringar som avses i 12 § 1 mom. en gång per år eller på begäran av det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president eller på ministeriets eget initiativ.

Huvudstaben ger försvarsministeriet årligen en redogörelse för den militära underrättelseverksamheten, dess art och omfattning samt hur den har inriktats. En redogörelse ska dessutom ges utan dröjsmål när försvarsministeriet ber om det.

3 kap.

**Samverkan med andra myndigheter och internationellt samarbete**

16 §

*Samarbete med skyddspolisen*

Militärunderrättelsemyndigheterna ska agera i samarbete med skyddspolisen för att underrättelsemyndigheternas uppgifter ska kunna skötas på ett ändamålsenligt sätt och i detta syfte, trots vad som föreskrivs om sekretess, ge skyddspolisen behövliga uppgifter.

17 §

*Samarbete med andra myndigheter och sammanslutningar*

Militärunderrättelsemyndigheterna ska enligt behov agera i samarbete med andra myndigheter för att den militära underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt.

Militärunderrättelsemyndigheterna kan för att genomföra sitt uppdrag agera i samarbete med sammanslutningar samt till andra myndigheter och sammanslutningar trots sekretessbestämmelserna lämna ut uppgifter, om utlämnandet av uppgifterna är nödvändigt med avseende på försvaret av landet eller för att skydda den nationella säkerheten.

I 76 och 77 § föreskrivs om utlämnande av information för brottsbekämpning.

18 §

*Samordning av hemlig informationsinhämtning*

Användningen av de metoder för underrättelseinhämtning om vilka det föreskrivs i denna lag ska vid behov samordnas för att säkerställa arbetssäkerheten för skyddspolisens, militärunderrättelsemyndigheternas och centralkriminalpolisens tjänstemän samt för att förhindra att de taktiska och tekniska metoder och planer som används vid hemlig informationsinhämtning avslöjas.

19 §

*Internationellt samarbete*

Militärunderrättelsemyndigheterna kan i enlighet med Finlands nationella intressen i anknytning till sina uppgifter eller för att skydda den nationella säkerheten

1) utbyta underrättelseuppgifter med utländska underrättelse- och säkerhetstjänster trots sekretessbestämmelserna, och

2) delta i internationellt samarbete i anknytning till inhämtandet och bedömningen av underrättelseuppgifter.

Om gemensam informationsinhämtning genomförs i samarbete med den stat, på vars territorium metoder för underrättelseinhämtning är avsedda att användas, ska militärunderrättelsemyndigheternas tjänstemän iaktta de begränsningar och villkor för användningen av metoderna för underrättelseinhämtning som staten i fråga ställer.

En behörig tjänsteman från en främmande stat har med ett beslut av Huvudstabens underrättelsechef rätt att på finskt territorium för skötsel av militärunderrättelsemyndigheternas uppgifter samarbeta med en tjänsteman vid en militärunderrättelsemyndighet samt under dennes uppsikt och övervakning använda de metoder för underrättelseinhämtning som avses i 20, 22, 41, 45, 49 och 63 §.

Huvudstabens underrättelsechef beslutar om deltagande i internationellt samarbete och om användning av metoderna för underrättelseinhämtning.

Vid utlämnande och mottagande av uppgifter enligt denna paragraf iakttas dessutom vad som särskilt anges om detta i internationella fördrag som är förpliktande för Finland eller föreskrivs i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004). Närmare bestämmelser om utlämnande av personuppgifter finns i lagen om behandling av personuppgifter inom Försvarsmakten.

4 kap.

**Metoder för underrättelseinhämtning**

*Systematisk observation, förtäckt inhämtande av information och teknisk observation*

20 §

*Observation och systematisk observation*

Med observation avses iakttagande av en viss person eller grupp av personer i hemlighet i underrättelsesyfte. Vid observation får en kamera eller någon annan motsvarande teknisk anordning trots 24 kap. 6 § i strafflagen (39/1889) användas för att göra eller uppta visuella iakttagelser.

Med systematisk observation avses annan än kortvarig observation av en person eller grupp av personer som med fog kan antas ha samband med ett underrättelseuppdrag.

Militärunderrättelsemyndigheterna får inrikta systematisk observation på ett objekt som avses i 2 mom., om detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

Observation och systematisk observation får inte riktas mot utrymmen som används för stadigvarande boende. Tekniska anordningar får inte användas vid observation eller systematisk observation riktad mot hemfridsskyddade platser enligt 24 kap. 11 § i strafflagen.

21 §

*Beslut om systematisk observation*

Beslut om systematisk observation ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Beslutet om systematisk observation får meddelas för högst sex månader åt gången.

Beslutet om systematisk observation ska fattas skriftligen. I beslutet ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,

2) den person eller grupp av personer som är föremål för åtgärden,

3) de fakta som förutsättningarna för och inriktningen av den systematiska observationen grundar sig på,

4) beslutets giltighetstid,

5) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar den systematiska observationen,

6) eventuella begränsningar och villkor för den systematiska observationen.

22 §

*Förtäckt inhämtande av information*

Med förtäckt inhämtande av information avses inhämtande av information genom kortvarig interaktion med en viss person eller grupp av personer där falska, vilseledande eller förtäckta

uppgifter används för att hemlighålla militärunderrättelsemyndigheternas tjänstemans uppdrag.

Militärunderrättelsemyndigheterna får använda förtäckt inhämtande av information för utförande av ett underrättelseuppdrag.

Förtäckt inhämtande av information är inte tillåtet i en bostad ens med bostadsinnehavarens medverkan.

23 §

*Beslut om förtäckt inhämtande av information*

Beslut om förtäckt inhämtande av information ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Beslutet om förtäckt inhämtande av information ska fattas skriftligen. I beslutet ska följande nämnas:

1) åtgärden och dess syfte samt det underrättelseuppdrag som ligger till grund för åtgärden,

2) den person eller grupp av personer som är föremål för åtgärden,

3) de fakta som förutsättningarna för och inriktningen av det förtäckta inhämtandet av information grundar sig på,

4) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar det förtäckta inhämtandet av information,

5) den planerade tidpunkten för genomförandet av åtgärden,

6) eventuella begränsningar och villkor för det förtäckta inhämtandet av information.

Beslutet ska vid behov ses över när omständigheterna förändras.

Om åtgärden inte tål uppskov, behöver ett beslut om förtäckt inhämtande av information inte upprättas i skriftlig form före åtgärden vidtas. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter att åtgärden har vidtagits.

24 §

*Teknisk avlyssning*

Med *teknisk avlyssning* avses att en viss persons eller persongrupps samtal eller meddelande som inte är avsett för utomstående och i vilket avlyssnaren inte deltar, trots 24 kap. 5 § i strafflagen 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 deltagarnas verksamhet.

Militärunderrättelsemyndigheterna får inrikta teknisk avlyssning på en person eller grupp av personer som befinner sig utanför ett utrymme som används för stadigvarande boende, om detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag. Avlyssningen kan riktas mot sådana utrymmen eller andra platser som det kan antas att en person eller grupp av personer som har samband med ett underrättelseuppdrag sannolikt befinner sig i eller på eller besöker.

25 §

*Beslut om teknisk avlyssning*

Beslut om teknisk avlyssning av en person som har berövats sin frihet ska fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättel-

seinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Om ärendet inte tål uppskov, får beslut om teknisk avlyssning fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller en annan tjänsteman till dess 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 annan teknisk avlyssning än den som avses i 1 mom. ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

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) det underrättelseuppdrag som ligger till grund för åtgärden,

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 med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar den tekniska avlyssningen,

6) eventuella begränsningar och villkor för den tekniska avlyssningen.

26 §

*Optisk observation*

Med *optisk observation* avses att man trots 24 kap. 6 § i strafflagen iakttar eller gör upptagningar av en viss person eller grupp av personer eller av ett utrymme eller någon annan plats med en kamera eller andra utplacerade tekniska anordningar, metoder eller programvaror.

Militärunderrättelsemyndigheterna får inrikta optisk observation på en person eller grupp av personer som befinner sig utanför ett utrymme som används för stadigvarande boende, om detta kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag. Observationen kan riktas mot utrymmen eller andra platser där det kan antas att den person eller grupp av personer som är föremål för observationen sannolikt befinner sig eller som de kan antas besöka.

27 §

*Beslut om optisk observation*

Beslut om optisk observation av en person som har berövats sin frihet ska fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Om ärendet inte tål uppskov, får beslut om optisk observation fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman till dess 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 annan optisk observation än den som avses i 1 mom. ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Tillstånd får ges och beslut fattas för högst sex månader åt gången.

I ett yrkande och ett beslut om optisk observation ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,

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 med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar den optiska observationen,

6) eventuella begränsningar och villkor för den optiska observationen.

28 §

*Teknisk spårning*

Med *teknisk spårning* avses 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.

Militärunderrättelsemyndigheterna får för utförande av ett underrättelseuppdrag rikta teknisk spårning mot föremål, ämnen eller egendom eller mot föremål, ämnen eller egendom som en sådan person som har samband med ett underrättelseuppdrag antas inneha eller använda.

Om syftet med teknisk spårning är att följa hur en person förflyttar sig genom att en spårningsanordning fästs i de kläder som personen bär eller i ett föremål som personen bär med sig (*teknisk spårning av en person*), får åtgärden genomföras bara om detta med fog kan antas vara av synnerlig vikt för erhållande av information med avseende på ett underrättelseuppdrag.

29 §

*Beslut om teknisk spårning*

Beslut om teknisk spårning av en person ska fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Om ärendet inte tål uppskov, får beslut om teknisk spårning av en person fattas av en av militärunderrättelsemyndigheterna för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman 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 från det att metoden för underrättelseinhämtning började användas.

Beslut om annan teknisk spårning än den som avses i 1 mom. ska fattas av en av militärunderrättelsemyndigheterna för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

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) det underrättelseuppdrag som ligger till grund för åtgärden,

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 med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar den tekniska spårningen,
6) eventuella begränsningar och villkor för den tekniska spårningen.

30 §

*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 behövliga med avseende på ett underrättelseuppdrag.

Genom teknisk observation av utrustning får inte inhämtas information om innehållet i ett meddelande som förmedlas och som avses i 32 § och inte heller om identifieringsuppgifter om ett sådant meddelande.

Militärunderrättelsemyndigheten kan ges tillstånd till teknisk observation av utrustning hos en statlig aktör för utförande av ett underrättelseuppdrag.

Militärunderrättelsemyndigheterna kan ges tillstånd till teknisk observation av utrustning hos någon annan än en statlig aktör, om detta med fog kan antas vara av synnerlig vikt för inhämtande av information med avseende på ett underrättelseuppdrag. Militärunderrättelsemyndigheterna kan rikta teknisk observation av utrustning mot en dator eller en liknande teknisk anordning som en sådan person som har samband med ett underrättelseuppdrag sannolikt använder eller mot dess programvara.

31 §

*Beslut om teknisk observation av utrustning*

Beslut om teknisk observation av utrustning ska fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Om ärendet inte tål uppskov, får beslut om teknisk observation av utrustning fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman till dess 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 för underrättelseinhämtning 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) det underrättelseuppdrag som ligger till grund för åtgärden,
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 med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar den tekniska observationen av utrustning,
6) eventuella begränsningar och villkor för den tekniska observationen av utrustning.

*Underrättelseinhämtning i telenät*

32 §

*Teleavlyssning*

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 avsett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät eller någon annan kommunikationsförbindelse avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och identifieringsuppgifterna i anslutning till det. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas ha samband med ett underrättelseuppdrag.

Militärunderrättelsemyndigheterna kan ges tillstånd till teleavlyssning av en statlig aktör för utförande av ett underrättelseuppdrag.

Militärunderrättelsemyndigheterna kan ges tillstånd till teleavlyssning av någon annan än en statlig aktör, om detta med fog kan antas vara av synnerlig vikt för att inhämta information med avseende på ett underrättelseuppdrag.

33 §

*Inhämtande av information i stället för teleavlyssning*

Om det är sannolikt att ett meddelande som avses i 32 § och dess identifieringsuppgifter inte längre är tillgängliga genom teleavlyssning, kan militärunderrättelsemyndigheterna beviljas tillstånd att inhämta informationen hos ett teleföretag eller en sammanslutningsabonnent, under de förutsättningar som anges i 32 §.

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 militärunderrättelsemyndigheterna beviljas tillstånd till inhämtande av information i stället för teleavlyssning, om de förutsättningar som anges i 32 § finns.

34 §

*Beslut om teleavlyssning och annat motsvarande inhämtande av information*

Beslut om teleavlyssning och om inhämtande av information i stället för teleavlyssning ska fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Tillstånd till teleavlyssning eller 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) det underrättelseuppdrag som ligger till grund för åtgärden,

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 eller inhämtande av information i stället för teleavlyssning,
5) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar utförandet av teleavlyssningen eller inhämtandet av information i stället för teleavlyssning,
6) eventuella begränsningar och villkor för teleavlyssningen eller inhämtandet av information i stället för teleavlyssning.

35 §

*Teleövervakning*

Med *teleövervakning* avses att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät eller som har mottagits till en sådan adress eller utrustning samt att lokaliseringsuppgifter om en teleadress eller teleterminalutrustning inhämtas.
Militärunderrättelsemyndigheterna kan ges tillstånd till teleövervakning av en teleadress eller teleterminalutrustning som en statlig aktör innehar eller annars använder för utförande av ett underrättelseuppdrag.
Militärunderrättelsemyndigheterna kan ges tillstånd till teleövervakning av en teleadress eller teleterminalutrustning som någon annan än en statlig aktör innehar eller annars använder, om detta kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

36 §

*Beslut om teleövervakning*

Beslut om teleövervakning ska fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Om ett ärende som gäller teleövervakning inte tål uppskov, får beslut om teleövervakning fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman till dess 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.
Militärunderrättelsemyndigheterna får för utförande av ett underrättelseuppdrag med en persons samtycke inrikta teleövervakning på en teleadress eller teleterminalutrustning som personen innehar.
Beslut om den teleövervakning som avses i 2 mom. ska fattas av Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.
Tillstånd får beviljas och beslut fattas för högst sex månader åt gången, och tillståndet eller beslutet kan 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) det underrättelseuppdrag som ligger till grund för åtgärden och syftet med åtgärden,
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 med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar teleövervakningen,

6) eventuella begränsningar och villkor för teleövervakningen.

37 §

*Inhämtande av basstationsuppgifter*

Med *inhämtande av basstationsuppgifter* avses inhämtande av information om teleterminalutrustningar och teleadresser som redan är eller kommer att bli registrerade i ett telesystem via en viss basstation.

Militärunderrättelsemyndigheterna kan beviljas tillstånd att inhämta sådana basstationsuppgifter som är behövliga med avseende på ett underrättelseuppdrag.

38 §

*Beslut om inhämtande av basstationsuppgifter*

Beslut om inhämtande av basstationsuppgifter ska fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Om ärendet inte tål uppskov, får beslut om inhämtande av basstationsuppgifter fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman till dess 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 för underrättelseinhämtning började användas.

Tillstånd beviljas för en viss tidsperiod.

I ett yrkande och i ett beslut om inhämtande av basstationsuppgifter ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden och syftet med åtgärden,
2) den basstation som 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 med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar inhämtandet av basstationsuppgifter,
6) eventuella begränsningar och villkor för inhämtandet av basstationsuppgifter.

39 §

*Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning*

Militärunderrättelsemyndigheterna får för utförande av ett underrättelseuppdrag med en teknisk anordning inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning.

Kommunikationsverket kontrollerar att den tekniska anordningen inte på grund av sina egenskaper orsakar skadliga störningar i ett allmänt kommunikationsnäts anordningar eller tjänster. Beslut om inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

40 §

*Installation och avinstallation av anordningar, metoder eller programvara*

En tjänsteman som är anställd vid en militärunderrättelsemyndighet har 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 sådana föremål, ämnen, egendom, utrymmen, platser av annat slag eller informationssystem som åtgärden riktas mot, om det behövs för användningen av nämnda metod för underrättelseinhämtning. För att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran har en tjänsteman vid en militärunderrättelsemyndighet då rätt att i hemlighet ta sig in i ovan nämnda objekt och i ett informationssystem och att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemets 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 används för stadigvarande boende endast om domstolen har gett tillstånd till det på yrkande av Huvudstabens underrättelsechef eller på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

*Täckoperationer och bevisprovokation genom köp*

41 §

*Täckoperation*

Med *täckoperation* avses planmässigt inhämtande av information om en viss person eller dennes verksamhet eller en grupp av personer eller dess 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.

Militärunderrättelsemyndigheterna får inrikta en täckoperation på en person eller grupp av personer, om användningen av täckoperationen är nödvändig för att få information med avseende på ett underrättelseuppdrag, och inhämtandet av information måste anses vara behövligt på grund av att den verksamhet som är föremål för underrättelseuppdraget är planmässig, organiserad eller yrkesmässig eller på grund av att det kan antas att verksamheten fortsätter eller upprepas.

En täckoperation får företas i en bostad endast om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden.

Militärunderrättelsemyndigheterna får inrikta en täckoperation på en person eller grupp av personer i ett datanät, om detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

42 §

*Framställning om och plan för en täckoperation*

I en framställning om täckoperation 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) det underrättelseuppdrag 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 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.

43 §

*Beslut om en täckoperation*

Beslut om en täckoperation ska fattas av Huvudstabens underrättelsechef. Beslut om en täckoperation som enbart ska genomföras i ett datanät ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Beslut om en täckoperation får meddelas för högst sex månader åt gången.

Beslut om en täckoperation ska fattas skriftligen. I beslutet ska följande nämnas:
1) den som föreslagit åtgärden,
2) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som ansvarar för genomförandet av täckoperationen,
3) identifikationsuppgifterna för de tjänstemän som genomför täckoperationen,
4) det underrättelseuppdrag som ligger till grund för åtgärden,
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) beslutets 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.

44 §

*Brottsförbud*

En tjänsteman vid en militärunderrättelsemyndighet som företar en täckoperation får inte begå brott eller ta initiativ till ett brott.

Om en tjänsteman vid en militärunderrättelsemyndighet som företar en täckoperation begår en trafikförseelse, en ordningsförseelse eller något annat jämförbart brott för vilket det föreskrivna straffet är ordningsbot, går tjänstemannen fri från straffansvar, om gärningen har varit nödvändig för att syftet med täckoperationen ska nås eller för att inhämtandet av information inte ska avslöjas.

45 §

*Bevisprovokation genom köp*

Med *bevisprovokation genom köp* avses ett köpeanbud eller ett köp av ett föremål, ett ämne, egendom eller en tjänst som en militärunderrättelsemyndighet gör i syfte att ta om hand eller hitta ett föremål, ett ämne eller egendom som har samband med ett underrättelseuppdrag.

Militärunderrättelsemyndigheterna får genomföra bevisprovokation genom köp, om det är nödvändigt för att få information med avseende på ett underrättelseuppdrag.

Den som genomför bevisprovokation genom köp får utföra bara sådant inhämtande av information som är nödvändigt för genomförandet av 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 denne inte annars skulle begå.

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.

46 §

*Beslut om bevisprovokation genom köp*

Beslut om bevisprovokation genom köp ska fattas av Huvudstabens underrättelsechef. Beslut om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten får fattas också av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

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) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den person som är föremål för bevisprovokationen,
3) de fakta som förutsättningarna för och inriktningen av bevisprovokationen genom köp 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 med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar bevisprovokationen genom köp,
8) eventuella begränsningar och villkor för bevisprovokationen.

47 §

*Plan för genomförande av bevisprovokation genom köp*

Över genomförandet av bevisprovokation genom köp 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.

48 §

*Beslut om genomförande av bevisprovokation genom köp*

Beslut om genomförande av bevisprovokation genom köp ska fattas skriftligen. Beslutet ska fattas av en sådan för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman som ansvarar för genomförandet av bevisprovokation genom köp.

I beslutet ska följande nämnas:

1) den av en militärunderrättelsemyndighet för uppdraget förordnade och med användningen av metoder för underrättelseinhämtning särskilt förtrogna militärjurist eller annan tjänsteman som fattade beslutet om bevisprovokationen samt beslutets datum och innehåll,
2) identifikationsuppgifter för de tjänstemän vid militärunderrättelsemyndigheterna 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 beslutet inte upprättas i skriftlig form före bevisprovokationen inleds. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter bevisprovokationen.

Vid förändrade omständigheter ska beslutet om genomförande av bevisprovokationen vid behov ses över.

*Användning av informationskällor*

49 §

*Användning av informationskällor*

Med *användning av informationskällor* avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av underrättelseuppdrag av personer som inte hör till en finsk myndighet (*informationskälla*).

Militärunderrättelsemyndigheterna får be att en för ändamålet godkänd informationskälla som har lämpliga personliga egenskaper, har registrerats och har samtyckt till informationsinhämtning, inhämtar den information som avses i 1 mom. (styrd användning av informationskällor), om det med fog kan antas att styrd användning av informationskällor är av synnerlig vikt för erhållande av information med avseende på ett underrättelseuppdrag.

Vid styrd användning av informationskällor får en informationskälla inte ombes 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 informationskällan 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 informationsinhämtningen.

Bestämmelser om tryggande av informationskällor finns i 75 §.

50 §

*Betalning av arvode till informationskällan*

Till en registrerad informationskälla kan betalas arvode. Av grundad anledning kan arvode betalas även till en oregistrerad informationskälla. Det finns särskilda bestämmelser om skatteplikt för arvodet.

51 §

*Beslut om styrd användning av informationskällor*

Beslut om styrd användning av informationskällor ska fattas av Huvudstabens underrättelsechef.

Beslut om styrd användning av informationskällor får meddelas för 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 med användningen av Försvarsmaktens underrättelsetjänsts metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som ansvarar för genomförandet av underrättelseuppdraget,

3) identifikationsuppgifterna för informationskällan,

4) det underrättelseuppdrag som ligger till grund för åtgärden,

5) syftet med inhämtandet av information och planen för genomförande av detta,

6) beslutets giltighetstid,

7) eventuella begränsningar och villkor för den styrda användningen av informationskällor.

När omständigheterna förändras ska beslutet vid behov ses över. Beslut om att styrd användning ska avslutas ska fattas skriftligen.

*Platsspecifik underrättelseinhämtning och kopiering*

52 §

*Platsspecifik underrättelseinhämtning*

Med platsspecifik underrättelseinhämtning avses underrättelseinhämtning för att hitta föremål, egendom, handlingar eller information eller utröna omständigheter i något annat utrymme än ett utrymme som används för stadigvarande boende eller ett utrymme beträffande vilket 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.

Militärunderrättelsemyndigheterna kan ges tillstånd till platsspecifik underrättelseinhämtning för utförande av ett underrättelseuppdrag.

53 §

*Beslut om platsspecifik underrättelseinhämtning*

Beslut om platsspecifik underrättelseinhämtning ska fattas av domstol, när den riktas mot en hemfridsskyddad plats eller mot en plats som allmänheten inte har tillträde till eller dit tillträdet för allmänheten har begränsats eller förhindrats under den tid då den platsspecifika underrättelseinhämtningen genomförs, på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Om det ärende som avses i 1 mom. inte tål uppskov, får Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman besluta om platsspecifik underrättelseinhämtning till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar från det att metoden för underrättelseinhämtning började användas.

Beslut om annan platsspecifik underrättelseinhämtning än den som avses i 1 mom. ska fattas av Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Tillstånd kan ges och beslut fattas för högst en månad åt gången.

I ett yrkande och i ett beslut om platsspecifik underrättelseinhämtning ska tillräckligt noggrant specificeras:
1) det underrättelseuppdrag som ligger till grund för åtgärden,
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 för den platsspecifika underrättelseinhämtningen.
När sakens brådskande natur kräver det får ett beslut om platsspecifik underrättelseinhämtning dokumenteras efter att den platsspecifika underrättelseinhämtningen har genomförts.

54 §

*Kopiering*

Militärunderrättelsemyndigheterna har rätt att kopiera ett dokument eller ett annat föremål för utförande av ett underrättelseuppdrag.
När kopieringen riktas mot någon annans än en statlig aktörs meddelande, är en förutsättning att detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

55 §

*Kopiering av försändelser*

Militärunderrättelsemyndigheterna har rätt att kopiera ett brev eller en annan försändelse innan den anländer till mottagaren.
När kopieringen av en försändelse riktas mot någon annans än en statlig aktörs meddelande, är en förutsättning att detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

56 §

*Kvarhållande av försändelser för kopiering*

Om det finns skäl att anta att ett brev eller någon annan försändelse, som får kopieras, 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 och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman förordna att försändelsen ska hållas kvar på verksamhetsstället i fråga, tills kopiering hinner utföras.
Förordnandet 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 har meddelat förordnandet när försändelsen har anlänt. Denne ska utan ogrundat dröjsmål besluta om kopiering.

57 §

*Beslut om kopiering*

Beslut om kopiering ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Beslutet ska fattas skriftligen.

Om ett ärende inte tål uppskov, får också någon annan än en sådan tjänsteman vid en militärunderrättelsemyndighet som avses i 1 mom. i ett enskilt fall besluta om kopiering, till dess att den tjänsteman som avses i 1 mom. har avgjort saken. Ärendet ska ges till den tjänsteman som avses i 1 mom. för avgörande så snart det är möjligt, dock senast 24 timmar efter det att metoden för underrättelseinhämtning började användas.

*Radiosignalspaning, underrättelseinhämtning som avser utländska datasystem och underrättelseinhämtning utomlands*

58 §

*Radiosignalspaning*

Med *radiosignalspaning* avses informationsinhämtning som riktas mot radiofrekventa elektromagnetiska vågor (radiovågor).

Försvarsmaktens underrättelsetjänst eller försvarsgrenarna kan rikta radiosignalspaning mot radiovågor som sänds från eller till en anordning utanför finskt territorium.

Med radiosignalspaning får information inte inhämtas om innehållet i andra än statliga aktörers meddelanden.

59 §

*Beslut om radiosignalspaning*

Beslut om radiosignalspaning ska fattas av Huvudstabens underrättelsechef. Beslutet ska fattas skriftligen.

60 §

*Underrättelseinhämtning som avser utländska datasystem*

Med *underrättelseinhämtning som avser utländska datasystem* avses att information inhämtas med datatekniska metoder från ett datasystem utanför Finland.

Försvarsmaktens underrättelsetjänst får inrikta underrättelseinhämtning som avser utländska datasystem på ett datasystem, om detta kan antas vara av synnerlig vikt för att inhämta information med avseende på ett underrättelseuppdrag.

Över genomförandet av underrättelseinhämtning som avser utländska datasystem ska en sådan skriftlig plan upprättas som innehåller väsentlig och tillräckligt detaljerad information för beslutsfattandet om och genomförandet av underrättelseinhämtning som avser utländska datasystem. När omständigheterna förändras ska planen vid behov ses över.

61 §

*Beslut om underrättelseinhämtning som avser utländska datasystem*

Beslut om underrättelseinhämtning som avser utländska datasystem ska fattas av Huvudstabens underrättelsechef. Beslutet ska fattas skriftligen.

I ett beslut om underrättelseinhämtning som avser utländska datasystem ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) föremål för åtgärden,
3) målet och genomförandeplanen för underrättelseinhämtning som avser utländska datasystem,
4) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar underrättelseinhämtning som avser utländska datasystem,
5) eventuella begränsningar och villkor för underrättelseinhämtning som avser utländska datasystem.

Militärunderrättelsemyndigheterna ska hålla försvarsministeriet informerat om pågående underrättelseinhämtning som avser utländska datasystem.

62 §

*Militär underrättelseinhämtning utomlands*

På militär underrättelseinhämtning utomlands och på användning av metoder för underrättelseinhämtning utomlands får, utöver vad som i denna lag föreskrivs om förbud mot militär underrättelseinhämtning som gäller ett utrymme som används för stadigvarande boende, tillämpas bestämmelserna i 58 § 3 mom., 76–77 §, 79–80 §, 82 § 2 mom., 84 och 86 § i denna lag.

Beslut om militär underrättelseinhämtning och användning av metoder för underrättelseinhämtning som sker utanför Finland ska fattas av Huvudstabens underrättelsechef.

I fråga om innehållet i ett beslut, en framställning och en plan som gäller användning av en metod för underrättelseinhämtning iakttas vad som i denna lag föreskrivs om framställningar, planer, yrkanden eller beslut.

*Informationsinhämtning som avser datatrafik*

63 §

*Behandling av tekniska data*

För inriktning av underrättelseinhämtning som avser datatrafik får Försvarsmaktens underrättelsetjänst 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 resultatet av den statistiska analysen får inte ingå sådan information genom vilken en enskild fysisk person kan identifieras.

Försvarsmaktens underrättelsetjänst ska förstöra insamlade och lagrade tekniska data om datatrafiken omedelbart efter att resultatet av den statistiska analysen har blivit klart.

64 §

*Beslut om behandling av tekniska data*

Beslut om behandling av tekniska data ska fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vid Försvarsmaktens underrättelsetjänst.

Tillstånd kan beviljas för högst tre månader åt gången.

I ett yrkande och i ett beslut som gäller behandlingen av tekniska data ska följande nämnas:

1) det geografiska område eller nätområde i fråga om vilket tekniska data i inkommande eller utgående datatrafik ska behandlas,

2) de delar av kommunikationsnätet där data söks,

3) den med användningen av Försvarsmaktens underrättelsetjänsts metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar behandlingen av tekniska data,

4) en plan för hur behandlingen av tekniska data ska genomföras.

65 §

*Underrättelseinhämtning som avser en statlig aktörs datatrafik*

Försvarsmaktens underrättelsetjänst kan med hjälp av automatisk databehandling i den datatrafik som överskrider Finlands gräns i kommunikationsnät inhämta information om en med avseende på ett underrättelseuppdrag väsentlig statlig aktörs datatrafik samt behandla den statliga aktörens kommunikation. Inhämtningen av information i datatrafiken grundar sig på användningen av sökbegrepp.

Försvarsmaktens underrättelsetjänst får behandla den information som inhämtats i datatrafiken automatiskt och manuellt.

Som sökbegrepp får inte användas uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland.

66 §

*Beslut om underrättelseinhämtning som avser en statlig aktörs datatrafik*

Beslut om underrättelseinhämtning som avser en statlig aktörs datatrafik ska fattas av domstol på yrkande av Huvudstabens underrättelsechef. Om ärendet inte tål uppskov, får Huvudstabens underrättelsechef besluta om underrättelseinhämtning som avser en statlig aktörs datatrafik till dess 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 underrättelseinhämtning som avser datatrafik började användas.

Tillstånd får beviljas för högst sex månader åt gången.

I ett yrkande och i beslut om underrättelseinhämtning som avser en statlig aktörs datatrafik ska följande nämnas:

1) det underrättelseuppdrag för vilket datatrafik inhämtas,

2) de sökbegrepp eller kategorier av sökbegrepp som ska användas i underrättelseinhämtningen och motiveringarna till dem,

3) den del av kommunikationsnätet som underrättelseinhämtningen inriktas på samt motiveringarna till inriktningen,

4) tillståndets giltighetstid med angivande av klockslag,

5) den med användningen av Försvarsmaktens underrättelsetjänsts metoder för underrättelseinhämtning särskilt förtrogna tjänsteman vid Försvarsmaktens underrättelsetjänst som leder och övervakar underrättelseinhämtning som avser en statlig aktörs datatrafik,

6) eventuella begränsningar och villkor för underrättelseinhämtning som avser en statlig aktörs datatrafik.

67 §

*Underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer*

Försvarsmaktens underrättelsetjänst kan med hjälp av automatisk databehandling i den datatrafik som överskrider Finlands gräns i kommunikationsnät inhämta information om datatrafiken hos sådana andra än statliga aktörer som är väsentliga med avseende på ett underrättelseuppdrag, om den underrättelseinhämtning som riktas mot datatrafiken hos andra än statliga aktörer kan antas vara nödvändig för att inhämta information med avseende på ett underrättelseuppdrag. Inhämtningen av information i datatrafiken grundar sig på användningen av sökbegrepp.

Som sökbegrepp får inte användas uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland.

Underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer får inte inriktas utgående från ett meddelandes innehåll, om det inte vid inriktningen används information som beskriver innehållet i ett sabotageprogram.

Försvarsmaktens underrättelsetjänst får behandla den information som inhämtats i datatrafiken automatiskt och manuellt.

68 §

*Beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer*

Beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer ska fattas av domstol på yrkande av Huvudstabens underrättelsechef. Om ärendet inte tål uppskov, får Huvudstabens underrättelsechef besluta om underrättelseinhämtning som avser datatrafiken hos andra än statliga aktörer till dess 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 underrättelseinhämtning som avser datatrafik började användas.

Tillstånd får beviljas för högst sex månader åt gången.

I ett yrkande och i beslut som gäller underrättelseinhämtning som avser datatrafiken hos andra än statliga aktörer ska följande nämnas:

1) det underrättelseuppdrag för vilket datatrafik inhämtas,
2) fakta som gäller föremålet för underrättelseinhämtningen,
3) de fakta som förutsättningarna för användning av underrättelseinhämtning som avser datatrafik grundar sig på,
4) de sökbegrepp eller kategorier av sökbegrepp som ska användas i underrättelseinhämtningen och motiveringarna till dem,
5) den del av kommunikationsnätet som underrättelseinhämtningen inriktas på samt motiveringarna till inriktningen,
6) tillståndets giltighetstid med angivande av klockslag,
7) den tjänsteman vid Försvarsmaktens underrättelsetjänst som leder och övervakar insamlingen och lagringen av kommunikationen,
8) eventuella begränsningar och villkor för underrättelseinhämtning som avser datatrafik.

69 §

*Genomförande av den koppling som behandlingen av tekniska data och underrättelseinhämtning som avser datatrafik förutsätter*

Den som utför kopplingen verkställer de tillstånd som avses i 64, 66 och 68 § och styr den datatrafik som rör sig i den i tillståndet avsedda delen av kommunikationsnätet till Försvarsmaktens underrättelsetjänst.

Den som utför kopplingen överlåter vidare till Försvarsmaktens underrättelsetjänst den datatrafik som rör sig i den del av kommunikationsnätet som stämmer överens med den i tillståndet avsedda anslutningen.

70 §

*Tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning*

Med tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning avses:

1) statistisk analys av tekniska data utifrån ett uppdrag som skyddspolisen har gett Försvarsmaktens underrättelsetjänst och sändande av analysen till skyddspolisen, samt

2) inhämtande med hjälp av automatiserad databehandling, i enlighet med ett tillstånd som domstolen beviljat skyddspolisen, av datatrafik som rör sig i en den del av ett kommunikationsnät som överskrider Finlands gräns och vidareöverlåtelse av de inhämtade uppgifterna till skyddspolisen.

Bestämmelser om det tekniska genomförandet av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning finns i 10 § i lagen om civil underrättelseinhämtning avseende datatrafik.

Försvarsmaktens underrättelsetjänst får inte för skyddspolisens räkning ta reda på ett meddelandes innehåll i samband med det tekniska genomförandet av underrättelseinhämtning som avser datatrafik.

71 §

*Utlämnande av uppgifter om ett skadligt datorprogram till företag och sammanslutningar*

Militärunderrättelsemyndigheterna får trots sekretessbestämmelserna till ett företag, en sammanslutning eller myndighet lämna ut uppgifter som inhämtats med hjälp av underrättelseinhämtning som avser datatrafik och som gäller ett skadligt datorprogram och dess verkningar, om utlämnandet av uppgifterna behövs med avseende på det militära försvaret, för att skydda den nationella säkerheten eller trygga företagets eller sammanslutningens intressen.

**Skyddande av militär underrättelseinhämtning samt tryggande av tjänstemän och informationskällor**

72 §

*Skyddande av militär underrättelseinhämtning*

Militärunderrättelsemyndigheterna får använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt upprätta och använda falska handlingar, när det är nödvändig för att förhindra att den militära underrättelseinhämtningen avslöjas.

En registeranteckning som avses i 1 mom. ska rättas när förutsättningarna enligt det momentet inte längre finns.

73 §

*Beslut om skyddande av militär underrättelseinhämtning*

Beslut om registeranteckningar och upprättande av handlingar enligt 72 § ska fattas av Huvudstabens underrättelsechef.

Beslut om annat skyddande än det som avses i 1 mom. ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Huvudstabens underrättelsechef ska föra förteckning över anteckningarna och handlingarna, övervaka användningen av dem samt se till att anteckningarna rättas.

74 §

*Tryggande av en tjänsteman som använder en metod för underrättelseinhämtning*

En för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman får besluta att en tjänsteman som ska genomföra förtäckt inhämtande av information, en täckoperation eller bevisprovokation genom köp samt förbereda eller genomföra användning av informationskällor ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att tjänstemannens säkerhet ska kunna tryggas.

Avlyssningen och observationen får upptas. Upptagningarna ska utplånas så snart de inte behövs för att trygga tjänstemannens 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.

75 §

*Tryggande av informationskällor*

Militärunderrättelsemyndigheterna kan 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 och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman får besluta att en informationskälla, om informationskällan ger sitt samtycke till detta, 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.

Huvudstabens underrättelsechef får besluta att en informationskälla ges, för användning i ett enskilt fall, falska, vilseledande och förtäckta uppgifter eller registeranteckning eller att falska handlingar upprättas för att användas av informationskällan, om det är nödvändigt för att skydda informationskällans liv och hälsa. En registeranteckning ska rättas när förutsättningarna enligt detta moment inte längre finns.

6 kap.

**Utlämnande av underrättelseuppgifter i vissa fall**

76 §

*Anmälan om en brottsmisstanke*

Militärunderrättelsemyndigheterna ska utan oskäligt dröjsmål anmäla till centralkriminalpolisen, om det medan en metod för underrättelseinhämtning används framkommer att ett sådant brott kan antas ha begåtts för vilket det föreskrivna strängaste straffet är fängelse i minst sex år. Genom beslut av Huvudstabens underrättelsechef får anmälan skjutas upp med högst ett år åt gången, om det är nödvändigt med avseende på försvaret av landet eller för att skydda den nationella säkerheten eller liv eller hälsa.

Militärunderrättelsemyndigheterna får anmäla ett begånget brott till centralkriminalpolisen, om det föreskrivna strängaste straffet för brottet är fängelse i minst tre år.

När det övervägs om en anmälan ska skjutas upp enligt 1 mom. eller en anmälan göras enligt 2 mom., ska betydelsen av utredningen av brottet med avseende på allmänna och enskilda intressen beaktas.

En för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman beslutar om den anmälan som avses i denna paragraf.

77 §

*Anmälan och lämnande av information i vissa fall*

Militärunderrättelsemyndigheterna ska utan dröjsmål anmäla till 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 inhämtats genom användning av en metod för underrättelseinhämtning får lämnas till behörig myndighet för förhindrande av ett sådant brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år.

När det övervägs om information ska lämnas enligt 2 mom. ska betydelsen av utredningen av brottet med avseende på allmänna och enskilda intressen beaktas.

Information som inhämtats genom användning av en metod för underrättelseinhämtning får alltid röjas som utredning som stöder att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada.

Huvudstabens underrättelsechef beslutar om den anmälan och om det lämnande av information som avses i denna paragraf.

78 §

*Anmälan om att förundersökning eller brottsbekämpning inleds*

Om en förundersökningsmyndighet, utgående från en anmälan eller lämnande av information som avses i detta kapitel, inleder en förundersökning eller vidtar en förundersökningsåtgärd eller om en brottsbekämpande myndighet inleder en åtgärd som syftar till att förhindra ett brott, ska förundersökningsmyndigheten eller den brottsbekämpande myndigheten innan förundersökningen inleds, förundersökningsåtgärden vidtas eller den brottsbekämpande åtgärden inleds till militärunderrättelsemyndigheterna anmäla detta.

7 kap.

**Förbud mot underrättelseinhämtning, utplåning av underrättelseinformation och underrättelse om användning av en metod för underrättelseinhämtning**

79 §

*Förbud mot underrättelseinhämtning*

Teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning, optisk observation, radiosignalspaning eller underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer får inte riktas mot sådan kommunikation eller information, som en part i kommunikationen inte får vittna om eller som han eller hon 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, optisk observation, radiosignalspaning eller underrättelseinhämtning som avser datatrafik 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.

Underrättelseinhämtning som avser datatrafik får inte riktas mot kommunikation där avsändaren och mottagaren befinner sig i Finland.

De förbud mot underrättelseinhämtning som avses i denna paragraf gäller dock inte sådana fall där en i 1 mom. avsedd person deltar i verksamhet som är föremål för militär underrättelseinhämtning och det också för hans eller hennes del har fattats beslut om teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning, optisk observation eller underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer.

80 §

*Kopieringsförbud*

Handlingar eller andra objekt som avses i 52 § får inte kopieras, 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 sekretessen, 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 sekretessen har föreskrivits samtycker till kopiering, eller

2) i 17 kap. 20 § 1 mom. i rättegångsbalken avsedd person samtycker till kopiering.

Handlingar eller data som innehas av ett teleföretag eller en sammanslutningsabonnent och som innehåller uppgifter om meddelanden som avses i 32 § 1 mom. eller innehåller identifieringsuppgifter som avses i 35 § 1 mom. eller basstationsuppgifter som avses i 37 § 1 mom. får inte kopieras.

81 §

*Utplåning av underrättelseinformation*

Information som erhållits med en metod för underrättelseinhämtning ska utplånas utan dröjsmål efter att det framgått att informationen inte behövs eller att den inte får användas för skötsel av uppdrag inom den militära underrättelseinhämtningen eller att informationen inte behövs med avseende på landets försvar eller för att skydda den nationella säkerheten.

Basstationsuppgifter som avses i 37 § ska utplånas när det har framgått att informationen inte behövs eller att den inte får användas för skötsel av uppdrag inom den militära underrättelseinhämtningen eller om informationen inte behövs med avseende på landets försvar eller för att skydda den nationella säkerheten.

En kopia som avses i 54 och 55 § ska utplånas utan dröjsmål, om det framgår att kopieringen har riktats mot material som omfattas av kopieringsförbud eller att informationen inte behövs med avseende på landets försvar eller för att skydda den nationella säkerheten.

Informationen får dock bevaras och lagras, om den behövs i de fall som anges i 76 eller 77 §.

82 §

*Avbrytande av teleavlyssning, teknisk avlyssning, radiosignalspaning, teknisk observation av utrustning och platsspecifik underrättelseinhämtning*

Om det framgår att teleavlyssningen riktas mot något annat meddelande än ett meddelande från eller till den som är föremål för tillståndet eller att den person som den tekniska avlyssningen riktas mot inte befinner sig i det utrymme eller på den plats av annat slag som avlyssnas, ska användningen av metoden för underrättelseinhämtning till denna del avbrytas så snart det är möjligt och de upptagningar som fåtts genom avlyssningen och anteckningarna om de uppgifter som fåtts genom den genast utplånas.

Skyldigheten att avbryta åtgärden och att utplåna upptagningarna och anteckningarna gäller också radiosignalspaning, om det framgår att radiosignalspaningen gäller innehållet i ett meddelande från någon annan än en statlig aktör, och teknisk observation av utrustning, om det framgår att den person som avses i 30 § 4 mom. inte använder den anordning som är föremål för observationen.

Om det medan platsspecifik underrättelseinhämtning pågår framgår att underrättelseinhämtningen har riktats mot information, om vilken det enligt 17 kap. 11, 13, 14, 16, 20, 21 § eller 22 § 2 mom. i rättegångsbalken föreligger skyldighet eller rätt att vägra vittna, ska underrättelseinhämtningen till denna del genast avbrytas och anteckningar om informationen och kopior av den genast utplånas.

Informationen får dock bevaras och lagras, om den behövs i de fall som anges i 76 eller 77 §.

83 §

*Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik*

Utöver vad som föreskrivs i 79 § 2 mom. ska information som erhållits genom underrättelseinhämtning som avser datatrafik utplånas utan dröjsmål, om det framgår att

1) båda parterna i kommunikationen befann sig i Finland när kommunikationen försiggick, eller

2) avsändaren, mottagaren eller den som upptar kommunikationen har skyldighet eller rätt att vägra vittna om informationen med stöd av de bestämmelser som anges i 79 § 1 mom.

För utplåningen svarar militärunderrättelsemyndigheterna. Om Försvarsmaktens underrättelsetjänst har lämnat uppgifterna till skyddspolisen vid ett tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning, svarar skyddspolisen för utplåningen.

Informationen får dock bevaras och lagras, om den behövs i de fall som anges i 76 eller 77 §.

84 §

*Avslutande av användningen av en metod för underrättelseinhämtning om vilken beslut har fattats i en brådskande situation och utplåning av uppgifter som erhållits genom den*

Om Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman i en i 25, 27, 29, 31, 36, 38, 53, 66 eller 68 § avsedd brådskande situation har beslutat att teknisk avlyssning, optisk observation, teknisk spårning av person, teknisk observation av utrustning, teleövervakning, inhämtande av basstationsuppgifter, platsspecifik underrättelseinhämtning, underrättelseinhämtning som avser en statlig aktörs datatrafik eller underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer 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.

Om en tjänsteman vid en militärunderrättelsemyndighet i en brådskande situation enligt 57 § 2 mom. har beslutat om kopiering, men en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman 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.

De uppgifter som avses i denna paragraf får dock användas för att anmäla ett i 76 § 1 mom. avsett brott eller för att förhindra ett i 77 § 1 mom. avsett brott.

85 §

*Användning av en uppgift som inte anknyter till ett underrättelseuppdrag*

En uppgift som inhämtats med en metod för underrättelseinhämtning men som inte anknyter till underrättelseuppdraget får användas vid utförandet av ett annat pågående eller kommande underrättelseuppdrag, om uppgiften hade fått inhämtas med samma metod för underrättelseinhämtning som den uppgift som inte anknyter till ett underrättelseuppdrag inhämtades med. Beslutet om användning av en uppgift som inte anknyter till ett underrättelseuppdrag ska fattas av domstol, om den har behörighet att besluta om den metod för underrättelseinhämtning med vilken uppgiften har fåtts eller av Huvudstabens underrättelsechef eller en för uppdraget förordnad militärjurist eller annan tjänsteman, om han eller hon har behörighet att besluta om användning av metoden för underrättelseinhämtning.

Om det ärende som avses i 1 mom. inte tål uppskov, får beslut om användningen av en uppgift som inte anknyter till ett underrättelseuppdrag fattas av en föruppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman till dess domstolen, Huvudstabens underrättelsechef eller den för uppdraget förordnade och med användningen av metoder för underrättelseinhämtning särskilt förtrogna militärjuristen eller andra tjänstemannen, vilka avses i 1 mom., har avgjort yrkandet om beviljande av tillstånd. Ärendet ska lämnas till domstolen, Huvudstabens underrättelsechef eller den för uppdraget förordnade och med användningen av metoder för underrättelseinhämtning särskilt förtrogna militärjuristen eller andra tjänstemannen, vilka avses i 1 mom., för avgörande så snart det är möjligt, dock senast inom 24 timmar från det användningen av en uppgift som inte anknyter till ett underrättelseuppdrag inleddes.

En uppgift som inte anknyter till ett underrättelseuppdrag får dock användas under samma förutsättningar som en uppgift får användas i de fall som avses i 76 § 1 mom. och 77 § 1 mom.

86 §

*Underrättelse om användning av en metod för underrättelseinhämtning*

Den person som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning och teknisk observation samt kopiering som riktas mot ett meddelande eller sådan kopiering av en försändelse som riktas mot ett meddelande ska utan dröjsmål underrättas om detta skriftligen efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts.

Underrättelseinhämtning som avser datatrafiken hos andra än statliga aktörer ska meddelas skriftligen till den person som varit föremål för underrättelseinhämtningen efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts och om innehållet i ett konfidentiellt meddelande från en viss person som befinner sig i Finland har retts ut manuellt vid behandlingen. Skyldighet att underrätta personen föreligger emellertid inte, om den in-

formation som inhämtats med underrättelseinhämtning som avser datatrafik har utplånats med stöd av 83 §.

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.

Om den som varit föremål för inhämtandet av information inte är identifierad vid utgången av den tid eller det uppskov som avses i 1–3 mom., ska han eller hon utan ogrundat dröjsmål skriftligen meddelas om användningen av en metod för underrättelseinhämtning när identiteten har utretts.

Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om underrättelsen.

På yrkande av Huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman får domstolen besluta att underrättelsen enligt 1 och 2 mom. till den som varit föremål för inhämtande av information får skjutas upp med högst två år åt gången, om det är motiverat för att trygga pågående användning av en metod för underrättelseinhämtning, med avseende på landets försvar eller för att garantera den nationella säkerheten eller skydda liv eller hälsa. Domstolen får besluta att underrättelsen helt ska utebli, om det är nödvändigt med avseende på landets försvar eller för att skydda den nationella säkerheten eller liv eller hälsa.

Den som 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 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 i 76 eller 77 § avsedd anmälan. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen (806/2011) iakttas.

Den som varit föremål för användningen av en metod för underrättelseinhämtning behöver inte underrättas om detta, om föremålet har varit en statlig aktör.

I fråga om handläggning av underrättelseärenden i domstol ska 113 § iakttas.

8 kap.

**Försvarsmaktens tjänstemäns och värnpliktigas deltagande i militär underrättelseinhämtning samt internationell verksamhet**

87 §

*Försvarsmaktens tjänstemäns deltagande i militär underrättelseinhämtning*

En tjänsteman vid Försvarsmakten som har fått tillräcklig utbildning i användningen av metoder för underrättelseinhämtning får under en militärunderrättelsemyndighets uppsikt och övervakning använda de metoder för underrättelseinhämtning som avses i 4 kap. för att inhämta information för ett underrättelseuppdrag. Dessa tjänstemän är underställda den militärunderrättelsemyndighet som utför underrättelseuppdraget.

88 §

*Befogenheter för en reservist som tjänstgör i enlighet med värnpliktslagen*

En reservist som deltar i en repetitionsövning i enlighet med värnpliktslagen (1438/2007) och som har fått tillräcklig utbildning får bistå militärunderrättelsemyndigheterna vid radiosignalspaning, underrättelseinhämtning som avser utländska datasystem, behandling av tekniska data och inriktning av underrättelseinhämtning som avser datatrafik.

En reservist som har förordnats till en i 32 § 3 mom. i värnpliktslagen avsedd repetitionsövning, som deltar i 82 § i den lagen avsedd extra tjänstgöring eller som har förordnats till tjänstgöring under mobilisering enligt 86 § i den lagen och som har fått tillräcklig utbildning får utöver det som föreskrivs i 1 mom. också använda systematisk observation, teknisk avlyssning, optisk observation, teknisk spårning och teknisk observation av utrustning samt underrättelseinhämtning som avser utländska datasystem för utförande av ett underrättelseuppdrag. I de situationer som avses i detta moment får vid underrättelseinhämtningen information om innehållet i ett meddelande inte inhämtas.

En reservist som i enlighet med 47 § i lagen om försvarsmakten har tagit avsked från en militärunderrättelsemyndighet och som deltar i en repetitionsövning enligt värnpliktslagen får använda de metoder för underrättelseinhämtning som avses i 4 kap.

Reservisten får använda de befogenheter som avses i denna paragraf endast under uppsikt och övervakning av en tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning.

89 §

*Deltagande i Försvarsmaktens internationella verksamhet*

Utöver vad som i denna lag föreskrivs om beslut i fråga om användning av metoderna för underrättelseinhämtning, får beslut om användning av metoder för underrättelseinhämtning när Försvarsmakten ger internationellt bistånd och i annan internationell verksamhet samt vid en militär krishanteringsinsats fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman eller av en sådan person som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning, som har tagit avsked från en militärunderrättelsemyndighet i enlighet med 47 § i lagen om försvarsmakten och som deltar i givandet av internationellt bistånd och i annan internationell verksamhet och har tagits i ett anställningsförhållande till Försvarsmakten eller står i ett tjänstgöringsförhållande enligt lagen om militär krishantering (211/2006).

En reservist som har fått tillräcklig utbildning i användningen av metoder för underrättelseinhämtning och som har tagits i ett anställningsförhållande till Försvarsmakten får använda metoder för underrättelseinhämtning under uppsikt och övervakning av en tjänsteman eller reservist som avses i 1 mom.

Huvudstabens underrättelsechef beslutar om en i denna paragraf avsedd persons deltagande i givandet av internationellt bistånd och i annan internationell verksamhet samt i militär krishantering samt om de tjänstemän och reservister som avses i 1 mom. och som får besluta om användningen av de metoder för underrättelseinhämtning som används i dessa.

90 §

*Tjänsteansvar för den som tjänstgör i enlighet med värnpliktslagen*

Bestämmelserna om straffrättsligt tjänsteansvar tillämpas på den som tjänstgör i enlighet med värnpliktslagen och använder en sådan metod för underrättelseinhämtning som avses i 87 eller 88 §.

91 §

*Skadeståndsansvar för den som tjänstgör i enlighet med värnpliktslagen*

För en skada som en reservist i tjänstgöring i enlighet med värnpliktslagen har orsakat svarar staten i enlighet med vad som föreskrivs i skadeståndslagen (412/1974).

På skadeståndsansvaret för en reservist i tjänstgöring i enlighet med värnpliktslagen tillämpas bestämmelserna om en värnpliktigs skadeståndsansvar i 4 kap. 2 § i skadeståndslagen.

9 kap.

**Yppandeförbud, skyldigheter och rättigheter som gäller teleföretag och dataöverförare samt användning och erhållande av information**

92 §

*Yppandeförbud*

En för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman får förbjuda en utomstående att röja sådana omständigheter om användningen av en metod för underrättelseinhämtning som denne fått kännedom om, om det är motiverat för skyddandet av underrättelseverksamheten. 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.

93 §

*Teleföretags biståndsskyldighet*

Ett teleföretag ska utan ogrundat dröjsmål göra de kopplingar i ett telenät som behövs för teleavlyssning och teleövervakning samt tillhandahålla militärunderrättelsemyndigheterna de uppgifter och redskap samt den personal som behövs för att teleavlyssning ska kunna utföras. Detsamma gäller också de situationer där en militärunderrättelsemyndighet genomför teleavlyssning eller teleövervakning med hjälp av en teknisk anordning.

94 §

*Dataöverförarens skyldighet att medverka till genomförandet och upprätthållandet av den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter*

En dataöverförare är skyldig att medverka till att den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter kan genomföras och upprätthållas genom att ge För-

svarsmaktens underrättelsetjänst de uppgifter som är nödvändiga för detta syfte och tillträde till de utrymmen där avsikten är att accesspunkten ska genomföras. Försvarsmaktens underrättelsetjänst ska genomföra accesspunkten så att detta orsakar så liten olägenhet som möjligt för dataöverföraren. Dataöverföraren har rätt att delta i åtgärderna för att genomföra accesspunkten.

Om den accesspunkt som avses i 1 mom. inte kan genomföras med medverkan av dataöverföraren, har Försvarsmaktens underrättelsetjänst rätt att genomföra accesspunkten i den del av ett kommunikationsnät som dataöverföraren administrerar. Om möjligt ska dataöverföraren vara på plats när den accesspunkt som förutsätts för underrättelseinhämtning som avser datatrafik genomförs.

95 §

*Dataöverförarens skyldighet att lämna uppgifter*

En dataöverförare ska utan obefogat dröjsmål, på en specificerad begäran av en till uppdraget av Försvarsmaktens underrättelsetjänst förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman lämna 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.

96 §

*Ersättningar till teleföretag*

Ett teleföretag har rätt att få ersättning av statens medel för direkta kostnader som orsakats av att företaget i enlighet med 93 § har bistått en militärunderrättelsemyndighet och lämnat uppgifter, så som föreskrivs i 299 § i lagen om tjänster inom elektronisk kommunikation. Den militärunderrättelsemyndighet som vidtagit åtgärden beslutar om utbetalning av ersättningen.

97 §

*Ersättningar till dataöverförare*

En dataöverförare har rätt att få ersättning av statens medel för direkta kostnader som orsakats av att överföraren i enlighet med 94 § har bistått en militärunderrättelsemyndighet och i enlighet med 95 § har lämnat uppgifter. Försvarsmaktens underrättelsetjänst beslutar om utbetalning av ersättningen.

98 §

*Sökande av ändring i ett ersättningsbeslut*

Omprövning av ett beslut om ersättning till ett teleföretag eller en dataöverförare får begäras på det sätt som anges i förvaltningslagen (434/2003).

Ett beslut som meddelats med anledning av en 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.

Förvaltningsdomstolen ska ge Kommunikationsverket tillfälle att bli hört.

99 §

*Avgifter för kopplingen*

Den som utför en koppling får ta ut avgifter av Försvarsmaktens underrättelsetjänst för tjänster som den har producerat med stöd av 4 kap. Avgifterna får inte överstiga beloppet av de totala kostnader som den som utför kopplingen orsakas av detta.

100 §

*Användning av uppgifter som lagras av teleföretag*

Utöver vad som i 157 § 1 mom. i lagen om tjänster inom elektronisk kommunikation föreskrivs om användning av lagrade uppgifter får lagrade uppgifter också användas för att inhämta information om verksamhet som avses i 4 § och är föremål för militär underrättelseinhämtning.

101 §

*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 militärunderrättelsemyndigheterna på begäran av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman rätt att av privata sammanslutningar få sådana uppgifter som i ett enskilt fall kan antas vara behövliga vid utredningen av sådan verksamhet som avses i 4 § och som kan antas vara av betydelse för att

1) identifiera eller nå en fysisk eller juridisk person som är föremål för militär underrättelseinhämtning, eller klarlägga personens kontaktuppgifter eller hur personen förflyttar sig,

2) inrikta användningen av en metod för underrättelseinhämtning på en viss person, eller

3) klarlägga ekonomisk verksamhet som bedrivs av en fysisk eller juridisk person.

Militärunderrättelsemyndigheterna har i ett enskilt fall på begäran rätt att av teleföretag och av sammanslutningsabonnenter få kontaktuppgifter för teleadresser som inte är upptagna i en offentlig katalog eller information som identifierar en teleadress eller teleterminalutrustning, om informationen behövs för utförande av ett underrättelseuppdrag. Militärunderrättelsemyndigheterna har motsvarande rätt att få information om utdelningsadresser av en sammanslutning som bedriver postverksamhet.

10 kap.

## Övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen

102 §

*Intern övervakning*

Chefen för Huvudstaben övervakar den militära underrättelseinhämtningen. Försvarsmaktens assessor svarar för den interna laglighetsövervakningen av den militära underrättelseinhämtningen.

103 §

*Övervakning som försvarsministeriet utför*

Försvarsministeriet övervakar den militära underrättelseverksamheten.

Försvarsministeriet har trots sekretessbestämmelserna rätt att få uppgifter om samhälleligt, ekonomiskt eller till sin allvarlighetsgrad betydande omständigheter som anknyter till den militära underrättelseinhämtningen.

104 §

*Extern övervakning av den militära underrättelseinhämtningen*

Försvarsministeriet ska årligen till riksdagens justitieombudsman och till underrättelseombudsmannen lämna en berättelse om hur metoderna för underrättelseinhämtning har använts och användningen övervakats samt om hur skyddandet av den militära underrättelseinhämtningen har använts och användningen övervakats.

105 §

*Anmälningar till underrättelseombudsmannen*

Militärunderrättelsemyndigheterna ska informera underrättelseombudsmannen om de beslut och tillstånd avseende metoder för underrättelseinhämtning som meddelats med stöd av denna lag så snart det är möjligt efter att de har meddelats.

Militärunderrättelsemyndigheterna ska så snart det är möjligt informera underrättelseombudsmannen om ett beslut som gäller

1) skyddandet av militär underrättelseinhämtning,
2) yppandeförbud,
3) uppskjutande av en anmälan som avses i 76 § 1 mom.

Vid anmälan av ett beslut som gäller en metod för underrättelseinhämtning ska särskild vikt fästas vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.

11 kap.

## Särskilda bestämmelser

106 §

*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.

107 §

*Granskning av upptagningar och handlingar*

Den tjänsteman som leder användningen av en metod för underrättelseinhämtning eller en av denne förordnad tjänsteman ska utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av metoden för underrättelseinhämtning.

108 §

*Undersökning av upptagningar*

De upptagningar som uppkommit vid användningen av metoder för underrättelseinhämtning får undersökas endast av domstolen och Huvudstabens underrättelsechef, en till uppdraget av militärunderrättelsemyndigheterna förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman eller av någon annan än en ovan avsedd tjänsteman vid en militärunderrättelsemyndighet som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning.

Dessutom får upptagningar på förordnande av Huvudstabens underrättelsechef också undersökas av en sakkunnig som står utanför militärunderrättelsemyndigheterna eller av en annan person som bistår vid informationsinhämtningen.

109 §

*Protokoll*

Över användningen av en metod för underrättelseinhämtning ska utan ogrundat dröjsmål upprättas ett protokoll.

110 §

*Tystnadsplikt*

I fråga om tystnadsplikt för tjänstemän som är anställda vid militärunderrättelsemyndigheterna tillämpas vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999), någon annanstans i lag och nedan i detta kapitel.

Tjänstemän som hör till en militärunderrättelsemyndighets personal får inte röja uppgifter som avslöjar identiteten hos en person som har lämnat information konfidentiellt eller deltagit i en täckoperation, om röjandet av uppgifterna kan äventyra den persons säkerhet som har

lämnat information konfidentiellt eller deltagit i en täckoperation, eller en närstående persons säkerhet.

Tystnadsplikten gäller också om röjandet av uppgifterna om identiteten kan äventyra redan avslutad, pågående eller framtida inhämtande av information.

Tystnadsplikt enligt 1–3 mom. har också den som utför ett underrättelseuppdrag under ledning och övervakning av militärunderrättelsemyndigheterna eller i ett anställningsförhållande till Försvarsmakten.

Tystnadsplikten gäller också efter det att anställningsförhållandet till militärunderrättelsemyndigheterna har upphört.

111 §

*Tystnadsrätt*

De som är hör till militärunderrättelsemyndigheternas personal är inte skyldiga att röja uppgifter om identiteten hos en person av vilken de i sitt anställningsförhållande har fått information konfidentiellt och inte heller om sekretessbelagda taktiska eller tekniska metoder.

Samma tystnadsrätt har den som utför ett underrättelseuppdrag under ledning och övervakning av en militärunderrättelsemyndighet eller bistår en militärunderrättelsemyndighet.

112 §

*Tjänstetecken*

Huvudstaben fastställer ett tjänstetecken som militärunderrättelsemyndigheternas tjänstemän ska medföra vid tjänsteutövning.

En tjänsteman vid en militärunderrättelsemyndighet ska vid utförandet av ett tjänsteuppdrag presentera sig som tjänsteman vid en militärunderrättelsemyndighet eller på begäran visa upp sitt tjänstetecken, om presentationen eller uppvisandet kan ske utan att åtgärden äventyras.

Andra identifikationer än den som avses i 1 mom. och som används vid tjänsteutövning inom militärunderrättelsemyndigheterna och som utvisar en tjänstemans ställning vid militärunderrättelsemyndigheterna godkänns av Huvudstabens underrättelsechef, som också beslutar om dess användning.

Militärunderrättelsemyndigheterna ska se till att en tjänsteman vid en militärunderrättelsemyndighet som har utfört ett tjänsteuppdrag vid behov kan identifieras.

113 §

*Förfarandet i domstol*

Ett tillståndsärende som gäller en metod för underrättelseinhämtning behandlas vid 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 metod för 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 i 4 kap. Beslutet ska meddelas omedelbart eller senast när behandlingen av sådana ärenden som gäller 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 behandlingen av det tidigare tillståndsärendet. Ärendet kan behandlas utan att nämnda tjänsteman 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 vid Helsingfors hovrätt. Klagan ska behandlas i brådskande ordning.

Vid handläggningen av ett ärende som gäller en metod för underrättelseinhämtning ska särskild vikt fästas vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.

114 §

*Begränsning av partsoffentlighet i vissa fall*

En person vars rättigheter eller skyldigheter saken gäller har inte, trots vad som föreskrivs i 11 § i lagen om offentlighet i myndigheternas verksamhet, rätt att få vetskap om informationsinhämtning enligt denna lag förrän underrättelse enligt 86 § har getts.

115 §

*Närmare bestämmelser*

Genom förordning av statsrådet får det utfärdas bestämmelser om

1) organiserandet av användningen och skyddandet av metoderna för underrättelseinhämtning,

2) dokumenteringen av åtgärderna för övervakningen,

3) de redogörelser som ska lämnas för övervakningen av den militära underrättelseinhämtningen,

4) det förfarande som gäller överföring av en uppgift som ska lämnas ut för brottsbekämpning,

5) organiserandet av samarbetet mellan militärunderrättelsemyndigheterna och skyddspolisen,

6) organiserandet av samarbetet mellan militärunderrättelsemyndigheterna och andra myndigheter,

7) organiserandet av samordningen av den hemliga informationsinhämtningen,

8) organiserandet av samordningen av underrättelseverksamheten.

Genom förordning av försvarsministeriet får det utfärdas bestämmelser om

1) organiserandet av övervakningen av den militära underrättelseinhämtningen inom försvarsförvaltningen,

2) organiserandet av militärunderrättelsemyndigheternas internationella samarbete.

116 §

*Ikraftträdande*

Denna lag träder i kraft den 20 .

_____

**2.**

# Lag

**om ändring av lagen om försvarsmakten**

I enlighet med riksdagens beslut
*fogas* till lagen om försvarsmakten (551/2007) en ny 8 a § som följer:

8 a §

*Militär underrättelseverksamhet*

Bestämmelser om Försvarsmaktens underrättelseverksamhet finns i lagen om militär underrättelseverksamhet ( /20 ).

---

Denna lag träder i kraft den 20 .

---

**3.**

# Lag

**om ändring av lagen om militär disciplin och brottsbekämpning inom försvarsmakten**

I enlighet med riksdagens beslut

*ändras* i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014) 13, 27, 36 och 86 § som följer:

13 §

*Huvudstabens behörighet att utfärda bestämmelser*

Samma befogenheter som tillkommer den disciplinära förman som avses i 12 § har även en förman i motsvarande uppdrag. Tjänstemän vid Försvarsmaktens underrättelsetjänst och huvudstabens underrättelseavdelning har inte i denna lag avsedda disciplinär förmans befogenheter. I övrigt bestämmer huvudstaben vem som ska anses vara en förman i motsvarande uppdrag. Dessutom kan huvudstaben, med avvikelse från föreskrifterna om de administrativa och militära befogenheterna, meddela föreskrifter om de inbördes disciplinära befogenheterna för de disciplinära förmän som är överordnade kommendören för ett truppförband.

27 §

*Förrättande av förundersökning*

Då ett brott som avses i militära rättegångslagen har kommit till en disciplinär förmans kännedom eller då det finns skäl att misstänka att ett sådant brott har begåtts, ska den disciplinära förmannen utan dröjsmål se till att förundersökning görs. Vid undersökningen tillämpas utöver denna lag vad som föreskrivs om förundersökning i brottmål.

Förundersökning ska också göras när en åklagare som avses i 4 § 1 mom. i militära rättegångslagen förordnar det.

Förundersökningen av ett brott som en tjänsteman vid Försvarsmaktens underrättelsetjänst misstänks för ska göras av huvudstaben så som föreskrivs i 35–41 §.

36 §

*Huvudstabens tjänstemän som sköter förundersökning*

Förundersökning görs och de befogenheter som har samband med detta utövas av tjänstemän vid huvudstabens juridiska avdelning enligt följande:

1) försvarsmaktens assessor och en militärjurist utövar de befogenheter som har föreskrivits för en polisman som hör till befälet och för en anhållningsberättigad tjänsteman,

2) överdetektiven och en yrkesmilitär som avses i lagen om försvarsmakten och som har förordnats till en förundersökningsuppgift eller en annan tjänsteman som har förordnats till uppgiften utövar de befogenheter som har föreskrivits för en polisman och utredare.

Enskilda förhör och andra undersökningsåtgärder kan ges i uppdrag åt en utredare enligt 28 § 3 mom.

Bestämmelser om tjänster, om utnämning till tjänster, förordnande till en uppgift och behörighetsvillkor för tjänster och uppgifter i fråga om de tjänstemän som avses i 1 mom. finns i lagen om försvarsmakten.

86 §

*Behörighet vid förebyggande och avslöjande av brott*

Vid försvarsmaktens förebyggande och avslöjande av brott sörjs det för att brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret förebyggs och avslöjas.

Det uppdrag som i 1 mom. föreskrivs för försvarsmakten begränsar inte skyddspolisens i lag föreskrivna behörighet.

Centralkriminalpolisen sörjer för att ett sådant brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och ett sådant brott som äventyrar syftet med det militära försvaret reds ut.

---

Denna lag träder i kraft den 20 .

---

**4.**

# Lag

**om ändring av 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät**

I enlighet med riksdagens beslut
*ändras* i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) 6 § 3 mom. som följer:

6 §

*Tillhandahållare av nät- och infrastrukturtjänster*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Tillhandahållaren av nät- och infrastrukturtjänster i säkerhetsnätet kan också vara ett dotterbolag som Suomen Erillisverkot Oy separat bildat för detta ändamål och som helt och hållet ägs av nämnda bolag. Dotterbolaget får inte ha som syfte att uppnå företagsekonomisk vinst. Dotterbolaget får också ha andra uppgifter, om så föreskrivs i lag. Vid skötseln av dessa uppgifter ska det i 2 mom. avsedda kravet på avskiljande av verksamheten beaktas.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

_____

Denna lag träder i kraft den 20 .

**5.**

# Lag

**om ändring av 92 b § i inkomstskattelagen**

I enlighet med riksdagens beslut
*ändras* i inkomstskattelagen (1535/1992) 92 b §, sådan den lyder i lag 528/2005, som följer:

92 b §

*Vittnesarvode, belöning för tips och arvode som ska betalas för användning av informationskälla*

Skattepliktig inkomst är inte
1) ersättning enligt lagen om bestridande av bevisningskostnader med statens medel (666/1972) av statens medel för kostnader för resa och uppehälle samt för ekonomisk förlust,
2) ersättning eller arvode som en myndighet betalar eller förmedlar för information som har bidragit till att ett brott har förebyggts eller utretts, en gärningsman har gripits eller den nytta som ett brott har medfört har återfåtts,
3) arvode som en myndighet betalar en i lagen om militär underrättelseverksamhet ( / ) och i polislagen (872/2011) avsedd informationskälla för inhämtande av uppgifter som är av betydelse för skötseln av underrättelseuppdrag.

_____

Denna lag träder i kraft den 20 .
_____

Helsingfors den 25 januari 2018

**Statsminister**

**Juha Sipilä**

Försvarsminister Jussi Niinistö

*Bilagor*
*Parallelltext*

**3.**

# Lag

**om ändring av lagen om militär disciplin och brottsbekämpning inom försvarsmakten**

I enlighet med riksdagens beslut
*ändras* i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014) 13, 27, 36 och 86 § som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 13 § | 13 § |
| *Huvudstabens behörighet att utfärda bestämmelser* | *Huvudstabens behörighet att utfärda bestämmelser* |
| Samma befogenheter som tillkommer den disciplinära förman som avses i 12 § har även en förman i motsvarande uppdrag. Huvudstaben bestämmer vem som ska anses vara en förman i motsvarande uppdrag. Dessutom kan huvudstaben, med avvikelse från föreskrifterna om de administrativa och militära befogenheterna, meddela föreskrifter om de inbördes disciplinära befogenheterna för de disciplinära förmän som är överordnade kommendören för ett truppförband. | Samma befogenheter som tillkommer den disciplinära förman som avses i 12 § har även en förman i motsvarande uppdrag. *Tjänstemän vid Försvarsmaktens underrättelsetjänst och huvudstabens underrättelseavdelning har inte i denna lag avsedda disciplinär förmans befogenheter. I övrigt bestämmer huvudstaben vem som ska anses vara en förman i motsvarande uppdrag.* Dessutom kan huvudstaben, med avvikelse från föreskrifterna om de administrativa och militära befogenheterna, meddela föreskrifter om de inbördes disciplinära befogenheterna för de disciplinära förmän som är överordnade kommendören för ett truppförband. |
| 27 § | 27 § |
| *Förrättande av förundersökning* | *Förrättande av förundersökning* |
| Då ett brott som avses i militära rättegångslagen har kommit till en disciplinär förmans kännedom eller då det finns skäl att misstänka att ett sådant brott har begåtts, ska den disciplinära förmannen utan dröjsmål se till att förundersökning görs. Vid undersökningen tillämpas utöver denna lag vad som föreskrivs om förundersökning i brottmål. | Då ett brott som avses i militära rättegångslagen har kommit till en disciplinär förmans kännedom eller då det finns skäl att misstänka att ett sådant brott har begåtts, ska den disciplinära förmannen utan dröjsmål se till att förundersökning görs. Vid undersökningen tillämpas utöver denna lag vad som föreskrivs om förundersökning i brottmål. |
| Förundersökning ska också göras när en | Förundersökning ska också göras när en |

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| åklagare som avses i 4 § 1 mom. i militära rättegångslagen förordnar det. | åklagare som avses i 4 § 1 mom. i militära rättegångslagen förordnar det.<br>*Förundersökningen av ett brott som en tjänsteman vid Försvarsmaktens underrättelsetjänst misstänks för ska göras av huvudstaben så som föreskrivs i 35–41 §.* |
| 36 § | 36 § |
| *Huvudstabens tjänstemän som sköter förundersökning* | *Huvudstabens tjänstemän som sköter förundersökning* |
| Förundersökning görs och de befogenheter som har samband med detta utövas av tjänstemän vid huvudstaben enligt följande:<br>1) försvarsmaktens assessor och en militärjurist utövar de befogenheter som har föreskrivits för en polisman som hör till befälet och för en anhållningsberättigad tjänsteman,<br>2) överdetektiven och en yrkesmilitär som avses i lagen om försvarsmakten och som har förordnats till en förundersökningsuppgift eller en annan tjänsteman som är anställd vid försvarsmakten och har förordnats till uppgiften utövar de befogenheter som har föreskrivits för en polisman och utredare. | Förundersökning görs och de befogenheter som har samband med detta utövas av tjänstemän *vid huvudstabens juridiska avdelning* enligt följande:<br>1) försvarsmaktens assessor och en militärjurist utövar de befogenheter som har föreskrivits för en polisman som hör till befälet och för en anhållningsberättigad tjänsteman,<br>2) överdetektiven och en yrkesmilitär som avses i lagen om försvarsmakten och som har förordnats till en förundersökningsuppgift eller en annan tjänsteman som har förordnats till uppgiften utövar de befogenheter som har föreskrivits för en polisman och utredare.<br>*Enskilda förhör och andra undersökningsåtgärder kan ges i uppdrag åt en utredare enligt 28 § 3 mom.* |
| Bestämmelser om tjänster, om utnämning till tjänster, förordnande till en uppgift och behörighetsvillkor för tjänster och uppgifter i fråga om de tjänstemän som avses i 1 mom. finns i lagen om försvarsmakten. | Bestämmelser om tjänster, om utnämning till tjänster, förordnande till en uppgift och behörighetsvillkor för tjänster och uppgifter i fråga om de tjänstemän som avses i 1 mom. finns i lagen om försvarsmakten. |
| 86 § | 86 § |
| *Behörighet vid förebyggande och avslöjande av brott* | *Behörighet vid förebyggande och avslöjande av brott* |
| Vid försvarsmaktens förebyggande och avslöjande av brott sörjs det för att brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret förebyggs och avslöjas.<br>Det uppdrag som i 1 mom. föreskrivs för försvarsmakten begränsar inte skyddspoli- | Vid försvarsmaktens förebyggande och avslöjande av brott sörjs det för att brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret förebyggs och avslöjas.<br>Det uppdrag som i 1 mom. föreskrivs för försvarsmakten begränsar inte skyddspoli- |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| sens i lag föreskrivna behörighet.<br>*Skyddspolisen* sörjer för att ett sådant brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och ett sådant brott som äventyrar syftet med det militära försvaret reds ut. | sens i lag föreskrivna behörighet.<br>*Centralkriminalpolisen* sörjer för att ett sådant brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och ett sådant brott som äventyrar syftet med det militära försvaret reds ut. |
| | _____ |
| | Denna lag träder i kraft den 20 . |
| | _____ |

**4.**

# Lag

**om ändring av 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät**

I enlighet med riksdagens beslut
*ändras* i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) 6 § 3 mom. som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 6 § | 6 § |
| *Tillhandahållare av nät- och infrastrukturtjänster* | *Tillhandahållare av nät- och infrastrukturtjänster* |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| Tillhandahållaren av nät- och infrastrukturtjänster i säkerhetsnätet kan också vara ett dotterbolag som Suomen Erillisverkot Oy separat bildat för detta ändamål och som helt och hållet ägs av nämnda bolag. Dotterbolaget *får inte ha andra uppgifter eller funktioner och det får inte ha som syfte att uppnå företagsekonomisk vinst.* | Tillhandahållaren av nät- och infrastrukturtjänster i säkerhetsnätet kan också vara ett dotterbolag som Suomen Erillisverkot Oy separat bildat för detta ändamål och som helt och hållet ägs av nämnda bolag. Dotterbolaget får inte ha som syfte att uppnå företagsekonomisk vinst. *Dotterbolaget får också ha andra uppgifter, om så föreskrivs i lag. Vid skötseln av dessa uppgifter ska det i 2 mom. avsedda kravet på avskiljande av verksamheten beaktas.* |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| | _____ |
| | Denna lag träder i kraft den 20 . |
| | _____ |

**5.**

# Lag

**om ändring av 92 b § i inkomstskattelagen**

I enlighet med riksdagens beslut
*ändras* i inkomstskattelagen (1535/1992) 92 b §, sådan den lyder i lag 528/2005, som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 92 b § | 92 b § |
| *Vittnesarvode och belöning för tips* | *Vittnesarvode,* ***belöning för tips och arvode som ska betalas för användning av informationskälla*** |
| Skattepliktig inkomst är inte<br>1) ersättning enligt lagen om bestridande av bevisningskostnader med statens medel (666/1972) av statens medel för kostnader för resa och uppehälle samt för ekonomisk förlust, *samt*<br>2) ersättning eller arvode som en myndighet betalar eller förmedlar för information som har bidragit till att ett brott har förebyggts eller utretts, en gärningsman har gripits eller den nytta som ett brott har medfört har återfåtts. | Skattepliktig inkomst är inte<br>1) ersättning enligt lagen om bestridande av bevisningskostnader med statens medel (666/1972) av statens medel för kostnader för resa och uppehälle samt för ekonomisk förlust,<br>2) ersättning eller arvode som en myndighet betalar eller förmedlar för information som har bidragit till att ett brott har förebyggts eller utretts, en gärningsman har gripits eller den nytta som ett brott har medfört har återfåtts,<br>*3) arvode som en myndighet betalar en i lagen om militär underrättelseverksamhet ( / ) och i polislagen (872/2011) avsedd informationskälla för inhämtande av uppgifter som är av betydelse för skötseln av underrättelseuppdrag.* |

Denna lag träder i kraft den 20 .