

Regeringens proposition till riksdagen med förslag till lag om ändring av lagen om militär underrättelseverksamhet och till lagar som har samband med den

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att lagen om militär underrättelseverksamhet, lagen om försvarsmakten, gränsbevakningslagen och strafflagen samt fem andra lagar ändras.

Det föreslås att de bestämmelser i lagen om militär underrättelseverksamhet som gäller underrättelseinhämtning som avser datatrafik ändras så att det vid underrättelseinhämtningen ska gå att fastställa sökbegreppen bättre så att underrättelseinhämtningen blir mer exakt inriktad. Militärunderrättelsemyndigheterna ges enligt förslaget möjlighet att behandla tekniska data i syfte att identifiera en del av ett kommunikationsnät eller identifiera dirigeringen av och ändringar i datatrafik. I den underrättelseinhämtning som avser datatrafik slopas förbudet mot att använda sökbegrepp som beskriver innehållet i ett meddelande samt förbudet mot att som sökbegrepp använda en teleterminalutrustning eller teleadress som finns eller kan förmodas finnas i Finland. I propositionen föreslås det att det inte längre ska underrättas om att underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer har använts.

I propositionen föreslås bestämmelser om en ny befogenhet inom den underrättelseinhämtning som avser datasystem med vars hjälp det ska vara möjligt att inhämta information om militär verksamhet eller om driften i Finland av datasystem som används för verksamhet som utgör ett allvarligt hot mot den nationella säkerheten.

Det föreslås att Gränsbevakningsväsendet ges behörighet att bistå militärunderrättelsemyndigheterna och på begäran av en militärunderrättelsemyndighet vidta vissa enskilda åtgärder i anslutning till användningen av vissa metoder för underrättelseinhämtning. Dessutom ska personer som inte är militärunderrättelsemyndigheter ges möjlighet att agera i avgränsade situationer och under ledning och övervakning av en militärunderrättelsemyndighet.

Det föreslås att informationsutbytet mellan militärunderrättelsemyndigheterna och vissa andra myndigheter utvidgas med tanke på utarbetandet av fullgöranderapporter och sådana situationer där det är nödvändigt att myndigheterna får information för utförandet av ett underrättelseuppdrag. I propositionen föreslås dessutom enstaka ändringar som hänför sig till författningsöversyn och ändringar som föranleds av preciseringsbehov som identifierats i den praktiska underrättelseverksamheten.

I lagen om försvarsmakten föreslås bestämmelser om inhämtande av information från allmänt tillgängliga källor och om användning av täckmantel vid sådant inhämtande av information.

Genom propositionen genomförs de föresatser om utveckling av underrättelselagstiftningen som ingår i regeringsprogrammet för statsminister Petteri Orpos regering.

De föreslagna lagarna avses träda i kraft så snart som möjligt.

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL	1
MOTIVERING.....	6
1 Bakgrund och beredning.....	6
1.1 Bakgrund.....	6
1.2 Beredning.....	7
2 Nuläge och bedömning av nuläget	7
2.1 Förändringarna i den säkerhetspolitiska miljön.....	7
2.1.1 Redogörelser	7
2.1.2 Underrättelsemyndigheternas översikter	10
2.1.3 Statsrådets redogörelse om underrättelselagstiftningen.....	12
2.1.4 Kommunikationsnät, datatrafik och underrättelseinhämtning som avser datatrafik	13
2.1.5 Datasystem.....	17
2.1.6 Förändringar i säkerhetsläget.....	17
2.2 Lagstiftning och praxis	18
2.2.1 Föremålen för militär underrättelseinhämtning och inriktningen av den	18
2.2.1.1 Föremålen för militär underrättelseinhämtning	18
2.2.1.2 Mekanismerna för att begränsa underrättelseverksamhet.....	22
2.2.2 Utlämnande av information om sabotageprogram	28
2.2.3 Installation och avinstallation av anordningar, metoder eller programvaror.....	28
2.2.4 Underrättelseinhämtning som avser datasystem i Finland	29
2.2.5 Teknisk observation av utrustning.....	30
2.2.6 Underrättelseinhämtning som avser datatrafik	31
2.2.7 Ingripande i verksamheten i ett informationssystem som äventyrar landets försvar och den nationella säkerheten	33
2.2.8 Underrättelseskyldigheten	39
2.2.9 Deltagande av utomstående i förhållande till en militärunderrättelsemyndighet i militär underrättelseverksamhet.....	43
2.2.10 Tryggande av informationskällor	47
2.2.11 Platsspecifik underrättelseinhämtning och kopiering	48
2.2.12 En militärunderrättelsemyndighets rätt att få uppgifter.....	49
2.2.13 Underrättelseinhämtning från öppna källor	50
2.2.14 Rekrytering hos Försvarsmakten	52
2.3 Bedömning av nuläget	56
2.3.1 Utlämnande av information om sabotageprogram	56
2.3.2 Installation och avinstallation av anordningar, metoder eller programvaror.....	56
2.3.3 Underrättelseinhämtning som avser datasystem i Finland	57
2.3.4 Teknisk observation av utrustning.....	59
2.3.5 Behandling av tekniska data om datatrafik.....	61
2.3.6 Sökbegreppen i underrättelseinhämtning som avser datatrafik	62
2.3.7 Ingripande i verksamheten i ett informationssystem som äventyrar landets försvar och den nationella säkerheten	63
2.3.8 Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik	67

2.3.9 Underrättelseskyldigheten	67
2.3.10 Deltagande i militär underrättelseinhämtning av en person som inte hör till en militärunderrättelsemyndighet	71
2.3.11 Tryggande av informationskällor	74
2.3.12 Platsspecifik underrättelseinhämtning och kopiering	75
2.3.13 En militärunderrättelsemyndighets rätt att få uppgifter	76
2.3.14 Inhämtande av information från allmänt tillgängliga källor	76
2.3.15 Rekryteringen vid Försvarsmakten	78
3 Målsättning	78
4 Förslagen och deras konsekvenser	79
4.1 De viktigaste förslagen	79
4.2 De huvudsakliga konsekvenserna	83
4.2.1 Ekonomiska konsekvenser	83
4.2.2 Konsekvenser för företagen	85
4.2.3 Konsekvenser för samhällsekonomin och näringslivet	87
4.2.4 Konsekvenser för informationshanteringen	89
4.2.5 Övriga konsekvenser för människor och samhälleliga konsekvenser	91
4.2.5.1 De grundläggande fri- och rättigheterna och de mänskliga rättigheterna	91
4.2.5.2 Jämlikhet och jämställdhet mellan könen	94
4.2.5.3 Myndigheternas verksamhet	94
4.2.5.4 Den nationella säkerheten och landets försvar	97
4.2.5.5 Informationssamhället och dataskyddet	99
4.2.5.6 Gränsöverskridande konsekvenser	99
5 Alternativa handlingsvägar	100
5.1 Handlingsalternativen och deras konsekvenser	100
5.2 Lagstiftning och andra handlingsmodeller i utlandet	102
5.2.1 Europeiska människorättskonventionen	102
5.2.2 Konventionen om medborgerliga och politiska rättigheter	109
5.2.3 Unionsrätten	110
5.2.4 Utländsk lagstiftning	113
5.2.4.1 Sverige	113
5.2.4.2 Norge	116
5.2.4.3 Danmark	118
5.2.4.4 Tyskland	119
5.2.4.5 Nederländerna	120
5.2.4.6 Cyberåtgärder på det internationella planet	121
6 Remissvar	122
6.1 Utlåtandena om arbetsgruppens betänkande	122
6.2 Utlåtandet av bedömningsrådet för lagstiftningen	129
7 Specialmotivering	131
7.1 Lagen om militär underrättelseverksamhet	131
7.2 Lagen om försvarsmakten	185
7.3 Strafflagen	189
7.4 Lagen om Finansinspektionen	190
7.5 Lagen om Enheten för utredning av grå ekonomi	190

7.6 Inkomstskattelagen	191
7.7 Gränsbevakningslagen.....	192
7.8 Lagen om behandling av personuppgifter vid Gränsbevakningsväsendet	193
7.9 Lagen om behandling av personuppgifter inom Försvarsmakten.....	193
8 Ikraftträdande	194
9 Förhållande till andra propositioner	195
10 Förhållande till grundlagen samt lagstiftningsordning.....	195
10.1 Allmänna utgångspunkter	195
10.2 Lagen om militär underrättelseverksamhet	197
10.2.1 De allmänna principer som begränsar militär underrättelse	197
10.2.2 Underrättelseinhämtning som avser datatrafik	198
10.2.3 De åtgärder som vidtas av en person utanför militärunderrättelsemyndigheten	217
10.2.4 Teknisk observation av utrustning.....	223
10.2.5 Användningen av en utomstående anordningar eller informationssystem	225
10.2.6 Omhändertagande och provtagning från ett ämne, egendom eller ett föremål.....	226
10.2.7 Värnpliktiga och andra som deltar i en övning.....	227
10.2.8 Underrättelseinhämtning som hänför sig till en statlig aktörs datasystem i hemlandet.....	228
10.2.9 Deltagande av en utländsk tjänsteman i militär underrättelseinhämtning	230
10.2.10 Tryggande av informationskällor	231
10.2.11 Andra omständigheter som ska bedömas	233
10.2.12 Skyddet för personuppgifter	235
10.3 Lagen om försvarsmakten.....	239
10.4 Exakthet, noggrann avgränsning och proportionalitet i fråga om inskränkningar av de grundläggande fri- och rättigheterna.....	244
10.5 Förslagen till bestämmelser i förhållande till Europadomstolens avgörandepraxis	247
10.5.1 Underrättelseinhämtning som avser datatrafik	247
10.5.2 Behandling av tekniska data och fastställande av sökbegrepp	249
10.5.3 Sökbegrepp som gäller innehållet i kommunikationen	250
10.5.4 Avstående av underrättelse av underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer	251
10.6 Förslagen till bestämmelser med tanke på EU-domstolens avgörandepraxis	252
10.7 Sammandrag	253
LAGFÖRSLAG.....	254
Lag om ändring av lagen om militär underrättelseverksamhet	254
Lag om ändring av lagen om försvarsmakten.....	270
Lag om ändring av 17 kap. 7 § i strafflagen	271
Lag om ändring av 71 d § i lagen om Finansinspektionen	271
Lag om ändring av 6 § i lagen om Enheten för utredning av grå ekonomi	272
Lag om ändring av 92 b § i inkomstskattelagen	272
Lag om ändring av gränsbevakningslagen	273
Lag om ändring av 32 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet.....	274
Lag om ändring av lagen om behandling av personuppgifter inom Försvarsmakten.....	274

BILAGA	276
Lag om ändring av lagen om militär underrättelseverksamhet	276
Lag om ändring av lagen om försvarsmakten.....	309
Lag om ändring av 17 kap. 7 § i strafflagen	310
Lag om ändring av 71 d § i lagen om Finansinspektionen	311
Lag om ändring av 6 § i lagen om Enheten för utredning av grå ekonomi	312
Lag om ändring av 92 b § i inkomstskattelagen	313
Lag om ändring av gränsbevakningslagen	314
Lag om ändring av 32 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet.....	315
Lag om ändring av lagen om behandling av personuppgifter inom Försvarsmakten.....	315

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Lagen om militär underrättelseverksamhet (590/2019) trädde i kraft den 1 juni 2019. Lagen innehåller centrala bestämmelser om militär underrättelseinhämtning, såsom befogenheter vid underrättelseinhämtning som avser datatrafik. Helheten av lagstiftning kring underrättelseverksamhet har fungerat på det avsedda sättet. I och med lagstiftningen kan det anses att hotlägesbilden har förbättrats till och med i avsevärd grad. Utöver myndigheternas utvidgade befogenheter har övervakningen av dessa genomförts effektivt och framgångsrikt. I och med att verksamheten startat och tekniken och den globala verksamhetsmiljön förändrats har det dock kommit fram ändringsbehov, som det inte varit möjligt att identifiera i samband med beredningen av den gällande lagen.

Med anledning av statsrådets redogörelse (RSk 70/2022 rd – SRR 11/2021 rd) om underrättelseverksamheten har riksdagen godkänt nedanstående ställningstagande enligt förvaltningsutskottets betänkande (FvUB 35/2022). I ställningstagandet förutsätter riksdagen att regeringen också i övrigt granskar underrättelselagstiftningens funktion, konsekvenser och eventuella ändringsbehov, ser till att lagstiftningen är uppdaterad i en föränderlig omvärld och säkerställer tillräckliga resurser för underrättelseverksamheten och tillsynen över den.

Dessutom har behoven av att ändra lagstiftningen identifierats även i den utredning över funktionen för lagstiftningen om militär underrättelseverksamhet vilken överlämnats till riksdagen.

Regeringsprogrammet för statsminister Petteri Orpos regering (avsnitt 10.1 Den nationella säkerheten och samhällets kriställighet stärks) innehåller flera föresatser som gäller utveckling av underrättelselagstiftningen. Lagstiftningen om underrättelseverksamhet är en del av landets försvar och skyddet av den nationella säkerheten.

Enligt regeringsprogrammet utvecklar regeringen underrättelselagstiftningen för att trygga myndigheternas funktionsförmåga med anledning av erfarenheterna av underrättelseverksamheten, den tekniska utvecklingen och Finlands Natomedlemskap. Underrättelselagstiftningen ses över i fråga om befogenheterna för underrättelseinhämtning samt rätten att få och lämna ut information så att den motsvarar kraven i den förändrade säkerhets- och cybermiljön.

Regeringen säkerställer att underrättelsebefogenheterna motsvarar den tekniska utvecklingen. Inom underrättelseverksamheten görs bland annat underrättelseinhämtning möjlig i sammanlänkad utrustning och sammanlänkade system samt genom användning av sökbegrepp i innehållet i meddelanden. Enligt regeringsprogrammet görs dessutom en bedömning av om underrättelsebefogenheterna ska utvidgas till utrymmen som används för boende av permanent natur.

Enligt regeringsprogrammet görs en bedömning av huruvida myndigheternas biståndsskyldighet ska utvidgas till tjänsteleverantörer i Finland, såsom datorhallsföretag. Möjligheten att föreskriva om en behörighet att behandla och utnyttja stora informationsresurser som fås från öppna källor utreds.

Enligt regeringsprogrammet föreskrivs under regeringsperioden en befogenhet att påverka utrustning eller programvara utomlands som används för sådant cyberspionage eller sådan cyberpåverkan som allvarligt äventyrar Finlands nationella säkerhet.

Enligt regeringsprogrammet föreskrivs därtill en rätt för Gränsbevakningsväsendet att använda prestationsförmågan för att stödja underrättelsemyndigheterna och rätt att lämna ut uppgifter till underrättelsemyndigheterna.

1.2 Beredning

Försvarsministeriet har den 28 augusti 2024 inrättat ett projekt för att bereda förslag till revidering av lagen om militär underrättelseverksamhet och lagar som har samband med den. I beslutet om att inrätta projektet har dess mandatperiod fastställts till tiden mellan den 29 augusti 2024 och den 1 juni 2025. Genom beslutet från den 26 maj 2025 har projektets mandatperiod förlängts fram till den 31 december 2025. För projektet inrättades en arbetsgrupp med representanter från försvarsministeriet, huvudstaben, inrikesministeriet och skyddspolisens. Arbetsgruppen omfattade företrädare från underrättelsetillsynsombudsmannens byrå och Gränsbevakningsväsendets stab som permanenta sakkunniga.

Ett remissförfarande ordnades om utkastet till regeringens proposition mellan den 27 november 2025 och den 16 januari 2026. Remissbehandlingen genomfördes via tjänsten utlåtande.fi. Utlåtandena om utkastet till regeringens proposition är offentligt tillgängliga i utlåtandetjänsten på adressen [utlatande.fi](https://www.utlatande.fi). Dessutom är utlåtanden om utkastet och projekthandlingarna tillgängliga på statsrådets webbplats under beteckningen PLM007:00/2024.

2 Nuläge och bedömning av nuläget

2.1 Förändringarna i den säkerhetspolitiska miljön

2.1.1 Redogörelser

Omvälvningarna i maktförhållandena i världspolitiken påverkar verksamhetsmiljön för Finlands försvar. Den allt hårdare strategiska konkurrensen och de globala motsättningarna mellan demokratier och auktoritära stater håller på att leda till att det multilaterala samarbetet splittras och regionaliseras. Konkurrensen Förenta staterna och Kina är en tävling om den ledande positionen i världen på det politiska, militära, ekonomiska och tekniska området. Ryssland har å sin sida intagit en konfrontatorisk hållning till Förenta staterna och de övriga västländerna, delvis i samarbete med Kina.

Förändringen i Finlands säkerhetsmiljö har beskrivits på heltäckande sätt i statsrådets redogörelse om förändringarna i den säkerhetspolitiska miljön från våren 2022¹ och försvarsredogörelsen för år 2024². Enligt redogörelserna har Rysslands invasion av Ukraina inneburit en grundläggande och långvarig förändring i Finlands och Europas omvärld och

¹ Redogörelse om förändringarna i den säkerhetspolitiska miljön. Statsrådets publikationer 2022:18.

<http://urn.fi/URN:ISBN:978-952-383-772-0>

² Statsrådets försvarsredogörelse. Försvarsministeriets publikationer 2024:5.

<http://urn.fi/URN:ISBN:978-951-663-423-7>

säkerhetspolitiska miljö. Upprätthållandet av samhällets resiliens, den nationella försvarsförmågan och den inre säkerheten får ökad betydelse för säkerheten i Finland.

Rysslands anfallskrig i Ukraina har fundamentala och långvariga konsekvenser för säkerhetsmiljön i Europa och Finlands närregioner. Ryssland har visat att landet inte respekterar andra staters suveränitet och territoriella integritet, landet har kränkt FN-stadgan och brutit mot den europeiska avtalsbaserade säkerhetsordningen.

Säkerhetsläget i Europa och Finland är allvarligare och svårare att förutse än någonsin efter kalla krigets slut och denna förändring bedöms bli långvarig. Enligt statsrådets redogörelse (2022) påverkar Rysslands krav och militära insatser för att förändra den europeiska säkerhetsarkitekturen också Finlands handlingsutrymme inom utrikespolitiken, säkerhetspolitiken och försvarspolitik. Finland ansökte om medlemskap i försvarsalliansen Nato den 17 maj 2022. Finland blev medlem i Nato den 4 april 2023.

Ryssland har inkluderat Finland och alla övriga EU-länder på en lista över så kallade ovänligt sinnade länder. Rysslands anfallskrig mot Ukraina har påverkat Finlands och Rysslands bilaterala relationer i grunden.

Trots att förändringarna i den säkerhetspolitiska miljön är långtgående och allvarliga riktas inget omedelbart militärt hot mot Finland. Finland har emellertid beredskap i det fall att väpnat våld eller hot om våld riktas mot Finland eller om våld används för politisk påtryckning. Aggressionen mot Ukraina visar att det är viktigt att ha en snabb insatsberedskap, förmåga att bemöta långvarig militär påtryckning och förmåga att avvärja en omfattande invasion från flera håll samtidigt. I statsrådets redogörelse (2022) konstateras det att ”om Finland ansöker om medlemskap i Nato bör man förbereda sig på omfattande och svårförutsägbara påtryckningar och risker, såsom ökade spänningar vid gränsen mellan Finland och Ryssland. Finland stärker sin beredskap för den eventualiteten att landet blir föremål för omfattande metoder för hybridpåverkan samt med tanke på att förhindra och reagera på påverkan”.

Rysslands invasion av Ukraina har haft omfattande negativa konsekvenser globalt och i synnerhet för säkerheten i Europa. Finland har reagerat på Rysslands anfallskrig mot Ukraina som en del av Europeiska unionen. Ryssland har utöver Ukraina kollektivt förklarat de västländer som deltar i de vidtagna motåtgärderna som sina fiender. Under rådande förhållanden har risken för underrättelseinhämtning och påverkan som riktas mot Finlands kritiska infrastruktur ökat både i den fysiska miljön och cybermiljön i och med Rysslands fullskaliga anfallskrig mot Ukraina och Finlands Natomedlemskap. Fastigheternas betydelse för den nationella säkerheten varierar avsevärt beroende på fastighetens användningsändamål, läge, de byggnader och konstruktioner som finns på fastigheten samt den kritiska infrastruktur och de strategiska objekt som eventuellt finns på fastigheten eller i närheten av den.

Säkerhetsläget i Europa och i Finlands närområden är instabilt och förändringarna i den säkerhetspolitiska miljön återspeglas också i gränssäkerhetsläget i Finland, vilket har synts till exempel som instrumentalisering av inresa från Rysslands sida. Detta har varit en av metoderna för att sträva efter att påverka Finlands nationella säkerhet och allmänna ordning. Finland måste förbereda sig på att påtryckningarna fortsätter under lång tid och antar mer omfattande och allvarligare former. Det bör finnas tillräcklig beredskap för hot mot den nationella säkerheten så att de kan förebyggas. Användningen av militära maktmedel mot Finland har i och med Finlands medlemskap i Nato fått en allt högre tröskel. När tröskeln för direkt väpnat våld är högre än tidigare accentueras andra metoder för breddspektrig påverkan. Således kan också fastighetsinnehavets betydelse för Finlands nationella säkerhet anses ha accentuerats ytterligare.

Ryssland använder metoder för bredspektrig påverkan – som omfattar hybridpåverkan och, i förekommande fall, användning av militära maktmedel – för att främja sina strategiska mål. Ryssland använder dessa metoder kontinuerligt också utan att tröskeln för en öppen konflikt överskrids, och landet kan flexibelt reglera intensiteten av påverkan och urvalet av metoder för att uppnå sina mål. Målet är bland annat att påverka mållandets enhetlighet, beslutsfattande och medborgaropinion samt att öka motsättningarna, skapa rädsla och fördunkla lägesbilden. För att stödja sina politiska målsättningar fortsätter Ryssland en aktiv underrättelseverksamhet och ett aktivt påverkansarbete, inte bara i fråga om traditionell informationsinhämtning och agentverksamhet utan också i datanäten. I sin verksamhet utnyttjar Ryssland inte bara de statliga myndigheterna utan också såväl företag och utbildnings- och forskningsinstitut som kriminella grupper och aktivister.

Möjligheterna att utnyttja cyberdomänen i fientligt syfte ökar när infrastrukturen och tekniken utvecklas och antalet användare ökar. Fientliga aktörer riktar ständigt underrättelseinhämtning i datanät, cyberspionage och cyberpåverkan mot västländerna och strävar efter att fysiskt påverka deras kritiska infrastrukturer. Bakom den fientliga aktiviteten ligger inte bara statliga aktörer utan i allt högre grad också icke-statliga aktörer som är politiskt motiverade eller statligt styrda.

Finland måste alltid och under alla säkerhetssituationer förbereda sig på användning av militära maktmedel mot Finland samt på hot om sådana och politiska påtryckningar. Hotet mot den nationella säkerheten kan konkretiseras under en väldigt lång tidsperiod på flera tiotals år och hotet mot den nationella säkerheten kan vara svår att konstatera under en viss tidpunkt. Finland sörjer för sin förmåga att reagera på utdragna militära påtryckningar samt långvarig och omfattande krigföring med nationella resurser och som en del av Nato. Militärt tvång och användning av militära maktmedel mot Finland kan förebyggas endast genom stark avskräckning och starkt försvar, vilket kräver tillräckliga resurser.

Finlands militära försvarssystem är en helhet som består av delsystem och som producerar de förmågor som det militära försvaret kräver. Försvarssystemets beredskap regleras så att den motsvarar hotnivån. Förmågan att övervaka alla domäner har utvecklats under de senaste åren. Särskilt rymd- och cyberdomänerna, informationsområdet, det elektromagnetiska spektrumet samt underrättelsesektorn kräver ett nära samarbete mellan förvaltningsområdena och andra centrala aktörer, inklusive internationella partner.

Försvarsmaktens gemensamma förmågor utvecklas så att de stöder den nationella försvarsförmågan och alliansens behov. Systemet för militär underrättelseinhämtning utvecklas för att möjliggöra tidig varning och stödjande av statsledningen, massiv och planmässig eldgivning samt för att utnyttja alliansens stöd. Genom långräckviddig påverkan med hög beredskap och stor räckvidd förebyggs och begränsas en angripares möjligheter att genomföra, leda och upprätthålla operationer.

Till Försvarsmaktens gemensamma förmågor hör militär underrättelseinhämtning, ledning, vapensystem med lång räckvidd, specialtrupper och logistik. Förändringarna i omvärlden och den tekniska utvecklingen har ställt nya krav på den militära underrättelseinhämtningen i synnerhet när det gäller inhämtande av information. Eftersom underrättelseinhämtningen i allt högre grad sker på nätet har befogenheterna enligt lagen om militär underrättelseverksamhet och utvecklandet av förmågan till underrättelseinhämtning ytterligare förbättrat förmågan att skapa en lägesbild och ge en tidig varning för reglering av beredskapen. Bedömningen av lagstiftningen om militär underrättelseverksamhet pågår kontinuerligt. En systematisk integrering av den militära underrättelseinhämtningen i Natos underrättelseverksamhet har kompletterat lägesbilden och utfärdandet av tidig varning. Ett nära samarbete mellan den

militära underrättelseinhämtningen och skyddspolisen utgör en stark grund för finländsk underrättelseinhämtning i alla sammanhang.

Försvarsförvaltningen bereder sig på att förebygga och bekämpa bredspektrig påverkan tillsammans med andra säkerhetsaktörer som en del av modellen för övergripande säkerhet och utvecklandet av totalförsvaret. För att kunna identifiera, förbereda för och möta påverkan krävs det att underrättelseverksamheten, specialtrupperna, cyberförsvaret, informationsförsvaret och den strategiska kommunikationen utvecklas i nationellt och internationellt samarbete.

Systemet för militär underrättelseverksamhet utvecklas så att det möjliggör tidig varning och stöd till statsledningen samt djupgående och planmässig eldanvändning utan dröjsmål och så att det möjliggör utnyttjande av alliansens stöd. Det nationella systemets kompatibilitet med de allierades system förbättras. Utöver interoperabilitet ligger fokus på att kombinera information och dela den med operativa användare. Förmågan att använda metoder för underrättelseinhämtning på ett mångsidigt sätt under normala förhållanden och undantagsförhållanden utvecklas.

Finland sörjer för utvecklingen av den nationella underrättelseverksamheten så att den motsvarar de ökade kraven och förändringarna i säkerhetsmiljön. Finland har beredskap att identifiera, förebygga och bekämpa spionage, hybridpåverkan, terrorism och militära hot i såväl den fysiska världen som cybervärlden. Utöver det redan etablerade internationella underrättelsesamarbetet deltar Finland aktivt i Natos underrättelsesamarbete.

2.1.2 Underrättelsemyndigheternas översikter

I Finlands militära underrättelseöversikt från år 2025³ konstateras att Finlands Natomedlemskap, det allt tätare internationella försvarssamarbetet och förändringen i den europeiska säkerhetsmiljön har ökat Rysslands behov av information om Finland. Underrättelsetjänsterna är intresserade av i synnerhet av Finlands genomförande av Natopolitiken, försvarssamarbetets utveckling, de internationella truppers verksamhet i Finland och utvecklingen av Natos staber och truppstrukturer. Under den tid som kriget i Ukraina har pågått, har dessutom behovet av att få fram information om försvarsindustrins produktionskapacitet och utvecklingen av Försvarsmaktens materiella prestationsförmåga accentuerats. Det primära underrättelsehotet mot försvarssystemet riktas mot Försvarsmaktens förmågor och användningsprinciper samt beredskap.

I Finlands närområde är de till Kolahalvön förlagda strategiska förmågorna, en obegränsad passage till Atlanten via de nordliga sjöförbindelserna samt det arktiska området centrala frågor för Ryssland. Ryssland strävar också efter att begränsa Natos verksamhet i Östersjöområdet och försvaga Finlands och Sveriges integration i Nato samt påverka innehållet i ländernas Natomedlemskap.

Ryssland har inlett en reform av sina väpnade styrkor som gäller militärdistrikten. Leningrads militärdistrikt, som verkar i Finlands närhet, planeras genomgå en märkbar förstärkning i framtiden. Då de ovan nämnda förändringarna har slutförts, växer styrkan för trupperna i Finlands närområde sannolikt från cirka 30 000 till cirka 80 000 soldater. Så länge

³ Finlands militära underrättelseöversikt 2025. Huvudstaben.

https://puolustusvoimat.fi/documents/1948673/2014902/PV_sotilastiedustelu_raportti_2025_web.pdf/4de8d666-6bff-642d-2d07-df71154b33bd?t=1737029070219

utnötningskriget i Ukraina fortsätter i sin nuvarande form, är det emellertid osannolikt att den militära styrkan i Finlands närområde kommer att öka nämnvärt. Efter att kriget i Ukraina avslutats, kommer Ryssland ändå sannolikt att prioritera sitt nordvästra område och sträva efter att verkställa reformerna i snabbare takt.

Ryssland strävar efter att påverka Finlands säkerhetspolitiska lösningar och låter förstå, att det skulle leda till ökade spänningar, ifall Natos infrastruktur skulle förläggas till Finland. Ryssland kommer sannolikt att öka användningen av alla metoder för bredspektrig påverkan i sin strävan att förorsaka splittring inom Nato och Europeiska unionen. Till dessa metoder hör cyber- och informationspåverkan, energipolitik, påverkan av energi- och övrig kritisk infrastruktur, styrning av immigranter och olika underrättelseoperationer.

Skyddspolisens översikt av den nationella säkerheten för år 2025⁴ innehåller en beskrivning av förändringen verksamhetsmiljön för underrättelseinhämtning. Enligt översikten bildar Ryssland och Kina det största underrättelsemässiga hotet för Finland. Ryssland försöker inhämta information i Finland med hjälp av såväl personbaserad underrättelseinhämtning som cyberunderrättelseinhämtning. Påverkan har alltid hört till de ryska underrättelse- och säkerhetstjänsternas verksamhet, men dess objekt och aktivitet har varierat beroende på det världspolitiska läget. Rysslands är i underrättelsehänseende särskilt intresserat av sina Natoanslutna gränsgrannar. När relationerna mellan Ryssland och västländerna har svalnat har Rysslands påverkansarbete tagit ett steg i allvarligare riktning. Landets sabotageverksamhet i Europa kan ses som ett exempel på detta.

De ryska underrättelsetjänsternas verksamhet mot Finland i cybermiljön har varit mycket aktiv redan i flera år, men de senaste åren har den ökat och blivit mer fokuserad. Det hot som rysk personbaserad underrättelseinhämtning utgör har dock inte minskat på lång sikt, eftersom Rysslands informationsbehov inte har försvunnit någonstans. I lägesbilden för både underrättelseinhämtning och bredspektrig påverkan har de proxyaktörer som olika stater använder fått en allt större roll. Statliga aktörer försöker sopa igen spåren efter sig genom mellanhänder, oavsett om det är fråga om Ryssland, Kina eller Iran. Med hjälp av proxyaktörer vill kraftmyndigheterna i diktatoriska länderna fördunkla verkligheten, göra det lättare att bestrida handlingar och skapa en ny typ av osäkerhet. Rekryteringen kan skötas i sociala medier och betalningen med kryptovalutor. Den som utför ett uppdrag vet inte nödvändigtvis själv för vems räkning han eller hon agerar.

De ryska säkerhets- och underrättelsetjänsterna har traditionellt haft permanent närvaro både i Finland och i andra länder. De som arbetat för underrättelsetjänsterna har i huvudsak gjort det under diplomatisk täckmantel, men Ryssland går alltmer in för att använda sig av mellanhänder och andra täckmantlar än diplomatin.

Den ryska underrättelsetjänstens närvaro i Finland och på annat håll i Europa har emellertid minskat betydligt i och med att underrättelseofficerare som arbetat under diplomatisk täckmantel utvisats som vedergällningsåtgärd mot anfallskriget. Andra bidragande orsaker är reserestriktionerna och att allt färre i Finland på grund av kriget vill ha ryska kontakter.

Det hot som rysk personbaserad underrättelseinhämtning utgör har dock inte minskat på lång sikt.

⁴ Översikt av den nationella säkerheten 2025. Skyddspolisens. <https://katsaus.supo.fi/etusivu>

Omvärldsförändringarna har även tvingat de ryska underrättelse- och säkerhetstjänsterna att ändra strategi. Ryssland går alltmer in för att använda sig av mellanhänder och andra täckmantlar än diplomatin. De kommer varken snabbt eller i stor skala att ersätta nyttan med diplomattäckmantel. Ryssland försöker även fortsatt att placera ut underrättelseofficerare som diplomater.

De ryska underrättelseaktörerna är i allt större utsträckning tvungna att bedriva sin verksamhet från Ryssland. Underrättelseinhämtningen kan gälla bosatta i Finland som uppehåller sig eller reser i Ryssland. Det är även möjligt att Ryssland använder osakliga metoder.

2.1.3 Statsrådets redogörelse om underrättelselagstiftningen

Statsrådet har gett en redogörelse om underrättelselagstiftningen⁵ år 2021. Enligt den ingår underrättelselagstiftningen i det samordnade genomförandet av målen för skyddet av den nationella säkerheten och försvaret och den har varit i kraft i en kort tid.

Utöandet av befogenheterna för underrättelseinhämtning bestäms av syftet med och föremålet för underrättelseinhämtningen, de allmänna och särskilda förutsättningarna för underrättelseinhämtning samt de allmänna principer som gäller verksamheten.

Det viktigaste målet med lagstiftningen om underrättelseinhämtning, nämligen att förbättra den nationella säkerheten, har förverkligats, och informationsinhämtningen om hot mot den nationella säkerheten och landets försvar har effektiviserats i och med de nya befogenheterna för underrättelseinhämtning. Det gemensamma mötet för ministerutskottet för utrikes- och säkerhetspolitiken och republikens president är en viktig aktör för beaktandet av utrikes- och säkerhetspolitiskt viktiga utvecklingsförlopp i underrättelseinhämtningen och uppföljningen av genomförandet av underrättelseinhämtningen. Finlands säkerhetsmiljö har efter att underrättelselagstiftningen antogs stått i en konstant förändring. Förändringarna utgör nya hot och kombinationer av hot för samhället och dess funktioner och medlemmar. Således är bedömningen av lagstiftningen en kontinuerlig, pågående process i och med att erfarenheterna av tillämpningen av underrättelselagstiftningen hela tiden blir mer omfattande. Man bereder sig även i fortsättningen på nya hot från många håll med hjälp av tidsenlig lagstiftning där de förutsättningar och förbehåll som följer av grundlagen beaktas.

I redogörelsen konstateras även att 66 § i lagen om militär underrättelseverksamhet innehåller bestämmelser om behandling av tekniska data som gäller underrättelseinhämtning som avser datatrafik, vilket föregår den egentliga underrättelseinhämtning som avser datatrafik. I bestämmelsen definieras inte kortvarigheten för insamlingen av tekniska data närmare, och definitionen fastställs i domstolen. Med beaktande av karaktären för de uppgifter som ska inhämtas och verksamheten har kortvarigheten visat sig vara problematisk.

Dessutom kan det tillstånd som behövs för insamling av tekniska data vara i kraft en kortare tid än den egentliga underrättelseinhämtningen som avser datatrafik, vilket leder till att tillståndsansökan ska förnyas. Tillståndets giltighetstid borde samordnas med tillståndstiden på sex månader för den egentliga underrättelseinhämtningen som avser datatrafik. För närvarande får information som fås genom behandling av tekniska data användas endast för att hitta en

⁵ Statsrådets redogörelse om underrättelselagstiftningen. Statsrådets publikationer 2021:94.
<http://urn.fi/URN:ISBN:978-952-383-500-9>

sådan del av ett kommunikationsnät som är av betydelse med tanke på underrättelseinhämtning som avser datatrafik.

Vid behandlingen av tekniska data har man dock identifierat att det fås uppgifter som kunde användas som sökbegrepp också vid egentlig underrättelseinhämtning som avser datatrafik samt vid preciseringen och utvecklingen av de sökbegrepp som ska användas.

Användningen av tekniska data som sökbegrepp skulle ytterligare begränsa den information som fås, noggrannare fokusera på objektet och effektivisera verksamheten. Detta skulle minska onödigt ingripande i individens rättigheter.

Vid utvecklandet av befogenheterna enligt lagstiftningen måste man beakta utvecklingen av ny teknik, som ofta tryggar integritetsskyddet bättre än tidigare, men som å andra sidan också möjliggör att olaglig verksamhet eller verksamhet som äventyrar den nationella säkerheten hemlighålls.

2.1.4 Kommunikationsnät, datatrafik och underrättelseinhämtning som avser datatrafik

Ett kommunikationsnätets fysiska struktur

I den digitaliserade världen och det digitaliserade samhället är samhällets funktion och människornas aktiviteter kraftigt beroende av datatrafiksystemet. Datatrafiksystemet består av ett stort antal anordningar som behövs för att förmedla datatrafik och större och mindre datatrafikkablar och ledningar som behövs för förmedlingen. De största kablarna, såsom havskablarna, består av fiberoptiska par (en fiber för, en annan fiber hämtar), medan mindre ledningar kan utgöras av kopparkablar. En vanlig havskabel innehåller 48 fiberpar.

Information som överförs i fiberoptiska kablar har omvandlats till ljus, medan informationen i kopparledningar överförs elektroniskt. Effektiviteten i överföringen av datatrafik i fiberoptiska kablar baserar sig på att data överförs med laser i fiberoptiska kablar och att det i en fiberoptisk kabel är möjligt att överföra data på tiotals olika våglängder, som syns i fibern som ljus av olika färger med hjälp av multiplextekniken (Dense Wavelength Division Multiplexing Access, DWMA). År 2025 är dataöverföringskapaciteten på en enskild våglängd i allmänhet omkring 100–400 Gbps i Finland. Således kan ett enskilt fiberoptiskt par i teorin transportera tiotals terabit per sekund. Även i fiberoptiska kablar försvagas ljuset, varför ett fiberoptiskt par med omkring 80–100 kilometers mellanrum ska anslutas till en anordning som finns längs rutten och som förstärker signalen.

Med mottagaren i ändan av det optiska överföringssystemet omvandlas våglängderna till kundsignaler, som styrs till en växel eller router. Med växlarna och routrarna behandlas bitflödet i datatrafiken på digital nivå och det styrs till följande anordningar i enlighet med routinginstruktionerna (routingprotokollet). Överföringen av en kundsignal från en optisk avsändare eller mottagare till en växlare och router kan ske längs en fiberoptisk linje eller en kopparkabel.

Datatrafik

För att en dator eller en annan terminalutrustning ska fungera på det önskade sättet och för att anordningarna ska fungera enligt de kommandon som ges till dem, förutsätts att information som kan tolkas visuellt av människan omvandlas till en binärkod. Binärsiffrorna 1 och 0 står för alternativen ”på” och ”av”. Binärsystemet är det enklaste sättet att behandla information i

elektroniska anordningar. Denna enkelhet gör binärsystemet till ett pålitligt och effektivt sätt att genomföra digital logik och beräkning.

På motsvarande sätt handlar datatrafik om ettor och nollor och datatrafik utgörs i praktiken av de konsekutiva siffrorna 1 och 0. Siffran 1 eller 0 bildar en bit och åtta bit bildar en byte. En byte representerar olika värden eller tecken, såsom en bokstav, en siffra eller ett specialtecken.

För att anordningarna i datatrafiksystemet och programmen i dessa ska kunna kommunicera och fungera tillsammans krävs olika tekniska regler och standarder, det vill säga protokoll. Till exempel datatrafikprotokollen (såsom HTTPS, som används av webbplatserna och TCP/IP, som används allmänt på internet) fastställer hur data överförs mellan näten, medan protokoll med lösenord och dataskydd (såsom SSL/TLS) säkerställer att informationen överförs säkert.

IP-protokollet (Internet Protocol) som används i omfattande grad kan granskas som ett närmare exempel. Det är ett datatrafikprotokoll som fungerar som grund för internet och andra datanät. Syftet med IP-protokollet är att möjliggöra att data överförs i ett nät mellan anordningarna, oberoende av var de finns fysiskt. De centrala egenskaperna för IP-protokollet är att:

- IP-adresser: Varje anordning som är ansluten till ett nät har en individuell IP-adress, som möjliggör att den identifieras och lokaliseras i nätet.
- Paketförsändelse: IP-protokollet delar upp data i små paket, som överförs via nätet till destinationen via den effektivaste ruten.
- Dirigering: Protokollet hjälper att hitta den bästa ruten, längs vilken ett datapaket förflyttas från avsändaren till mottagaren.

Till exempel i en situation där en person vill skicka ett fotografi med en storlek på 2–3 megabyte, måste bildfilen i typfallet delas upp i omkring 2 000 paket. Den anordning som används av avsändaren bildar ett paket, i vilket de behövliga uppgifterna för att styra paketet till mottagaren antecknas. Dessa uppgifter är bland annat den IP-adress med vilken den mottagande anordningen identifieras och den använda applikationen, såsom en webbtjänst, en e-postserver, en mobil anordning som tar emot ett videosamtal eller en plattform för innehållsdelening. Varje enskilda paket går längs den snabbaste och effektivaste ruten för varje enskilda paket till sin destination.

I datatrafik används dock ofta inte endast ett protokoll, utan flera behövs för att möjliggöra en pålitlig dataöverföring. På grund av detta kombineras IP-protokollet med TCP-protokollet (tillsammans TCP/IP-protokollet). Genom att använda TCP-protokollet fås utöver IP-protokollets egenskaper dessutom följande egenskaper:

- Hantering av dataöverföringen: TCP ansvarar för att dela upp data i mindre paket och för att sammanställa dessa i rätt ordning för mottagaren.
- Felkontroll: TCP granskar att alla paket mottagits och korrigerar eventuell fel som skett i dataöverföringen.
- Pålitlighet: Om något paket försvinner på vägen, skickar TCP det på nytt och säkerställer att dataöverföringen är komplett.

Till exempel i en situation där en användare vill öppna en webbplats, skickar terminalutrustningen således en begäran genom att använda TCP-protokollet, som delar upp

begäran i paket. IP-protokollet ansvarar för att dirigera paketen till rätt webserver. Webbserverns TCP-protokoll tar emot paketen, sammanställer dem till ett paket och sänder tillbaka svaret på samma sätt. Efter användning av flera protokoll och utbyte av data mellan anordningarna ser användaren den önskade webbplatsen på skärmen på sin terminalutrustning.

På det sätt som det beskrivna exemplet om TCP/IP-protokollparet redogör för, används ofta ett stort antal olika protokoll – för att smidiggöra dataöverföringen utgörs paketen ofta av flera protokollager. De olika lagren har olika användningssyften – ett lager kan beskriva till vilken anordning meddelande är avsett, ett annat hur trafiken har krypterats. I synnerhet i komplexare dataöverföringssystem eller i arrangemang med återförsäljning av förbindelser kan det finnas flera tiotals protokollager. För att trafiken ska dirigeras på behörigt sätt till mottagaren förutsätts behandling av alla lager. För att säkerställa interoperabiliteten mellan olika system iakttar protokollen oftast internationella standarder.

Varje datasystem lämnar ett eget individuellt digitalt fotavtryck i datatrafiken beroende på hur systemet kommunicerar, hur ofta det gör det och med vem samt på datatrafikens form. Således är det möjligt att även utan innehållet i kommunikationen, genom att analysera tekniska data om informationssystemets datatrafik få mycket information om informationssystemet och dess funktion. Identifiering av ett datasystem från datatrafikflödet förutsätter inte nödvändigtvis någon genomgång av kommunikationens innehåll eller annan information som omfattas skyddet för privatlivet enligt 10 § i grundlagen, utan information kan fås redan från den tekniska dirigerings trafiken och trafiken mellan andra system och anordningar.

De centrala tekniker som används i analysen utgörs av till exempel en analys av utflödet i datatrafiken. I ett datasystems datatrafik finns det vissa regelbundenheter, såsom fördelningen av paketstorleken i datatrafiken, den tidpunkt då datatrafik ankommer, datatrafiksessionernas längd och den kvantitativa variationen i datatrafiken. Till exempel ser datatrafikflöden som producerats av databas- och internetserverar olika ut.

Datasystemen kommunicerar även enligt en viss regelbundenhet. I datasystemen finns det ofta tidsinställda processer, pulsintervaller och synkroniseringsfigurer. Utifrån datatrafikflödet kan det direkt utredas att det inte producerats av en mänsklig användare.

Även de tidigare beskrivna protokollen påverkar datatrafikens struktur. De protokoll som används påverkar hur till exempel IP-paketen bildas, vilket för egen del påverkar hur datatrafikflödet ser ut och hurudant dess regelbundenhet är.

På det sätt som konstaterats i beskrivningen av ett datatrafiknät består ett modernt kommunikationsnät av flera transporterande fibrer och anordningar som förenar dessa. De centrala anordningarna är routrar.

Oftast är avsändaren av ett datatrafikpaket och mottagaren inte i direkt kontakt med varandra. I så fall finns det mellan anordningarna en eller flera routrar, det vill säga en anordning som planerats för att dirigera datatrafiken. Routrarna granskar de datatrafikpaket som inkommer till dem och överför antingen paketen till deras mottagare, om routern är direkt kopplad till mottagaren, eller styr paketen till följande router, som finns närmare mottagaren. Routrarna kommunicerar sinsemellan via routingprotokoll, såsom BGP (Border Gateway Protocol) eller IS-IS (Intermediate System to Intermediate System). Med routingprotokollet utbyts information om via vilken rutt olika IP-adresser kan nås bäst. Detta innebär att datatrafikpaket som gäller ett enskilt meddelande i elektronisk kommunikation, såsom ett skickat fotografi, inte går längs samma rutt till mottagaren, utan de överförs längs den rutt som är effektivast och snabbast för

varje enskilda paket fram till mottagaren. Således rör sig inte ett helt meddelande ens som konsekutiva datatrafikpaket i en del av ett kommunikationsnät.

Krypteringen av datatrafik

Enskilda personer och vissa aktörer strävar efter att hemlighålla sin datatrafik så långt som möjligt. Kryptering handlar om tekniker där kommunikation i ett nät ändras till sådan form att utomstående inte kan läsa eller redigera den till exempel utan rätt krypteringsnyckel. Genom kryptering säkerställs framför allt att endast mottagarna ser innehållet, informationen inte kan ändras utan att detta märks, avsändaren och mottagaren är de rätta och att sändning av ett meddelande inte kan förbjudas senare.

En central metod för att kryptera datatrafik är VPN-tjänster (Virtual Private Network). En av VPN-tjänsternas egenskaper är så kallad inkapsling av kommunikationen, där exempelvis ovan beskrivna IP-paket paketeras till nya IP-paket. Vid så kallad inkapsling finns uppgifterna om det egentliga meddelandets mottagare och avsändare således inne i ett annat meddelande, det vill säga i ett eller flera IP-paket.

Via VPN-tjänsterna skapas även andra virtuella interna nät för olika organisationers bruk. Genom ett virtuellt internt nät kan företrädarna för en organisation vara verksamma i olika delar av världen och ändå använda organisationens egna system på samma sätt som då de sitter på ett kontor.

Underrättelseinhämtning som avser datatrafik

Underrättelseverksamhet beskrivs ofta som läggande av pussel. Metoderna för underrättelseinhämtning kompletterar varandra och genom dem är det möjligt att inhämta olika former av information för att kunna lägga ett metaforiskt pussel. För att helheten ska kunna utredas, förutsätter detta ofta till en början att helhetsramarna utreds till exempel genom underrättelseinhämtning som avser datatrafik.

Underrättelseinhämtning som avser datatrafik har på grund av dess särdrag en viktig funktion att komplettera andra metoder för underrättelseinhämtning och möjliggöra användningen av sådana. Dess processuella särdrag möjliggör att anordningar som hotar landets försvar och den nationella säkerheten lokaliseras och att aktörerna bakom hoten identifieras. Observationer som gjorts genom underrättelseinhämtning som avser datatrafik är i många fall en nödvändig förutsättning för att metoder för underrättelseinhämtning som baserar sig på en annan inriktningslogik överhuvudtaget ska kunna användas.

Vid underrättelseinhämtning som avser datatrafik hänför sig underrättelseinhämtningen till en datatrafikkabel som överskrider Finlands gräns och de fiberoptiska par som löper i denna. Fysiskt sett styrs med andra ord ljus, som motsvarar ettor och nollor, från de fiberoptiska kablarna till ett datatrafiksystem. Genom att tolka binärkoden bildar anordningarna byte och utifrån dessa byte paket. Paketen bildar till slut ett helt meddelande, såsom en bild, eller en del av den. Även utan meddelandets innehåll kan väsentlig information fås om paketen, såsom information om meddelandets avsändare och mottagare.

Egentlig underrättelseinhämtning som avser datatrafik baserar sig på användning av sökbegrepp. I grund och botten baserar sig ett sökbegrepp på en serie av ettor och nollor, vilken i systemet jämförs med den datatrafik som inkommit till systemet. Om sifferserierna är enhetliga, kan denna datatrafik, närmare sagt paketen, granskas mer ingående. Föremålet för

granskningen är till exempel om datatrafikpaketet innehåller ett meddelande, vem som varit parter i meddelandet och varifrån meddelandet kommer. Ökningen av den elektroniska kommunikationen och krypteringen har lett till att en allt större del av paketflödet i datatrafiken anknyter till annat än meddelandets betydelseinnehåll.

Slutresultatet av den närmare analysen kan användas till exempel i underrättelserapporter och för att närmare rikta underrättelseinhämtningen samt för att fastställa nya sökbegrepp.

2.1.5 Datasystem

Ett datasystem kan definieras som ett system där information behandlas och används i ett visst syfte. Granskat ur en teknisk synvinkel kombinerar det anordningar, programvaror och regler på så sätt att information kan lagras, användas samt sändas och tas emot.

I synnerhet under de senaste 20 åren har den tilltagande takten inom den tekniska utvecklingen lett till att den information som används av människor och organisationer i praktiken inte lagras i en enskild anordning. Det nuvarande informationssamhället baserar sig på datanät, servrar avsedda för att lagra och behandla information, olika terminalutrustningar som används av människor samt en helhet som utgörs av sensorer avsedda för automation och minidatorer. Även de hot som avvärjs av en militärunderrättelsemyndighet fungerar till centrala delar genom att utnyttja dessa system.

Ett datasystem handlar med andra ord inte om en enskild anordning eller programvara, utan i den moderna världen bildas helheter av ett stort antal samverkande anordningar och programvaror. I sista hand finns det ofta kedjor av ett stort antal anordningar och programvaror bakom en tjänst som används med en enskild anordning.

2.1.6 Förändringar i säkerhetsläget

På det sätt som lagts fram i statsrådets utrikes- och säkerhetspolitiska redogörelse påverkar omvälvningarna i maktförhållandena i världspolitikens verksamhetsmiljön för Finlands försvar. Den allt hårdare strategiska konkurrensen och de globala motsättningarna mellan demokratier och auktoritära stater håller på att leda till att det multilaterala samarbetet splittras och regionaliseras. Konkurrensen Förenta staterna och Kina är en tävling om den ledande positionen i världen på det politiska, militära, ekonomiska och tekniska området. Ryssland har å sin sida intagit en konfrontatorisk hållning till Förenta staterna och de övriga västländerna, delvis i samarbete med Kina.

Det i hög grad digitaliserade och nätverkande samhället är en fast del av cyberverksamhetsmiljön. Denna miljö har skapat en ny möjlighet för staterna att uppnå sina mål med nya metoder. Dessa mål kan vara bland annat att stärka den egna politiken och synen samt att försvaga demokratin i andra stater genom att påverka kritiska funktioner i samhället, såsom val, kritisk infrastruktur eller informationsförmedling. Denna verksamhet beskrivs ofta med termerna hybridpåverkan eller omfattande påverkan.

Den i omfattande grad digitaliserade världen som är sammanflätad i nätverk öppnar en möjlighet även för en ny typ av hotverksamhet, såsom lågintensiva cyberoperationer och avancerade ihållande cyberhotsaktörer. Den först nämnda innebär verksamhet som i den internationella rättens kontext inte kan ses som en väpnad attack eller användning av militära maktmedel; det kan anses handla om att på allmänspråk orsaka en olägenhet. Den senare nämnda handlar om ett obemärkt permanent cyberhot som begås från hög nivå och som hänför sig till exempelvis kritisk infrastruktur och en stat och vars mål är exempelvis spionage, inhämtande av information

eller övertagande av ett systemet exempelvis för att uppnå politiska mål. Det centrala är att även om aktörens enskilda åtgärder kan avvärjas, fortsätter den hotande aktören sin verksamhet och riktar sannolikt sin verksamhet på nytt mot Finland.

Den tekniska utvecklingen möjliggör för cyberhotsaktörerna rentav industrialiserade och automatiserade angreppskedjor. Detta innebär att attackernas snabbhet och mängd ökar och att aktörerna automatiserar inläsningen av dataskyddsluckor, lateraltrafiken och analys- och utpressningsverktygen för data. De geopolitiska spänningarna styr såväl lågintensiva cyberoperationer som avancerade ihållande cyberhotsaktörer.

På grund av detta ska Finland sörja för utvecklingen av den nationella underrättelseverksamheten så att den motsvarar de ökade kraven och förändringarna i säkerhetsmiljön. Finland ska ha beredskap att identifiera, förebygga och bekämpa spionage, hybridpåverkan, terrorism och militära hot i såväl den fysiska världen som cybervärlden. Utöver det redan etablerade internationella underrättelsesamarbetet deltar Finland aktivt i Natos underrättelsesamarbete.

2.2 Lagstiftning och praxis

2.2.1 Föremålen för militär underrättelseinhämtning och inriktningen av den

2.2.1.1 Föremålen för militär underrättelseinhämtning

I 4 § i lagen om militär underrättelseverksamhet finns det bestämmelser om föremålen för militär underrättelseinhämtning. Av föremålen kan endast en del anses utgöra exklusiva föremål för militär underrättelseinhämtning, medan en del av föremålen är av sådan natur som delvis är överlappande med civil underrättelseinhämtning.

Föremål som uteslutande gäller militär underrättelseinhämtning handlar framför allt om militär verksamhet. Begreppet militär verksamhet har dock inte fastställts genom och det är inte heller känt att begreppet behandlats heller i den juridiska litteraturen (RP 203/2017 rd, s. 189). Den enda juridiska beskrivningen av militär verksamhet finns i regeringspropositionen om den upphävda lagen om försvarsmakten (402/1974) (RP 172/1999 rd). Den interna synvinkel som tillägnats i förarbetena till denna lag har styrt till att förstå begreppet bland annat som en strategisk, operativ och taktisk planering som gäller rikets territoriella integritet, planering av upprätthållande och utveckling av försvarsberedskapen, upprätthållande av det krigstida ledningssystemet, militär underrättelseinhämtning, den krigstida organisationen och beslut om den fastställda styrkan, placering av personal och förordnande till en krigstida uppgift samt utrustande av de krigstida trupperna och planering av underhållet samt förberedande åtgärder för dessa.

Ovan beskrivna beskrivning av militär verksamhet gäller i sig inte i en kontext av militär underrättelseinhämtning, eftersom intresset hänför sig till en främmande stats militära verksamhet i den. I en sådan extern granskning betraktas som militär verksamhet 1) statlig verksamhet och icke-statlig verksamhet av militärt organiserade trupper, 2) verksamhet som anknyter till militära maktmedel, såsom beväpning och krigsmateriel eller 3) annan verksamhet som jämföras med dessa och som bedrivs av trupper som använder militär kraft (RP 198/2017 rd, s. 35 och FvUU 7/2018 rd s. 4).

Statlig verksamhet härrör från verksamhet som bedrivs av en främmande stats väpnade styrkor eller från därmed jämförbar verksamhet som bedrivs av en internationell militär allians eller organisation, medan icke-statlig verksamhet avser sådan militärt organiserad, beväpnad eller

utrustad verksamhet som inte har ovan avsedda statliga ursprung eller där ett sådant ursprung inte kan identifieras. Typiskt för militär verksamhet är stora trupper, 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. Dessutom kräver militär verksamhet ofta kraftig ekonomisk resursallokering, som i regel endast stater har råd med (RP 203/2017 rd, s. 189).

Enligt 4 § 1 mom. 1 punkten i lagen om militär underrättelseverksamhet omfattar föremålen för den militära underrättelseinhämtningen verksamhet som bedrivs av en främmande stats väpnade styrkor och av med dem jämförbara organiserade trupper samt förberedelse för sådan verksamhet. Verksamheten ska vara av militär natur. Trupper som är jämförbara med en främmande stats väpnade styrkor ska bedömas enligt hur organiserad verksamheten är, vilka resurser trupperna har och hurdan verksamheten är i ett övergripande perspektiv (FsUB 9/2018 rd, s. 10).

Den avsedda verksamheten har inte avgränsats till att gälla endast verksamhet som riktas mot Finland, utan militärunderrättelsemyndigheten ska kunna inhämta information i omfattande grad om verksamhet som bedrivs av främmande staters väpnade styrkor eller av med dem jämförbara organiserade trupper även då detta inte orsakar något militärt hot för Finland. Utifrån den inhämtade informationen strävar man efter att strukturera, minska och även utnyttja osäkerhetsfaktorer i den säkerhetspolitiska miljön i försvaret av landet och i förberedelser för en kris (RP 203/2017 rd, s. 189–190).

Ett annat centralt mål är att ge en förhandsvarning till underrättelseinhämtningens klienter. En fientligt sinnad stat strävar ofta efter att genomföra sitt påverkansarbete på så sätt att målstaterna inte nödvändigtvis har full visshet om det handlar om en målinriktad och styrd operation eller ej. Utifrån objektiv information som fås i rätt tid får statsledningen mer svängrum då olika påtryckningsmetoder hänför sig till Finland. På grund av detta bevakas olika händelser och utvecklingscykler på ett övergripande sätt.

Det står klart att militär underrättelseverksamhet i enlighet med Försvarmaktens uppgifter ska riktas mot ett yttre hot mot Finland. Den militära underrättelseinhämtningens uppgiftsfält omfattar inte Finlands interna angelägenheter, såsom en statsintern konflikt eller påverkan i det demokratiska samhällslivet, såsom en generalstrejk. Situationer som organiserats eller i övrigt stötts av en främmande stats väpnade styrkor eller av med dem jämförbara organiserade trupper så att de ser ut som statsintern turbulens ska dock avskiljas från detta.

Verksamhet enligt punkten omfattar utöver egentlig militär verksamhet och verksamhet som bedrivs av grupper som kan jämföras med väpnade styrkor även förberedelse av verksamheten samt militära planer och avsikter. Information som är central för Finlands landsförsvar kan även fås från konflikter mellan andra stater eller en främmande stats militära övningar.

Förberedelserna och planerna täcker även exempelvis socialpolitiskt beslutsfattande och militär planerings- och utvecklingsverksamhet samt utveckling och upphandling av vapensystem. Förberedelserna och planerna kan även hänföra sig till att underblåsa intern turbulens i målstaten. Målet för en fientlig stat kan även vara att inleda en statskupp eller revolution annanstans än i Finland.

I 4 § 1 mom. 2 punkten i lagen om militär underrättelseverksamhet föreskrivs att föremålet för militär underrättelseverksamhet kan är militär underrättelseverksamhet av militär verksamhet, vilken riktar sig mot Finlands försvar. Enligt den internationella rätten åtnjuter varje suveräna stat territoriell integritet och politiskt oberoende i förhållande till andra stater. De flesta staterna

tolererar verksamhet som bedrivs av underrättelsemyndigheterna från främmande stater fram till en viss punkt.

Med utländsk militär underrättelseverksamhet avses sådan verksamhet som bedrivs av en främmande stat och vars mål är att inhämta information för att främja den egna statens intressen eller skada Finland eller en annan främmande stat och som den stat som är föremål för underrättelsen har ett särskilt intresse att sekretessbelägga. Föremålet för en främmande stats underrättelseinhämtning kan vara till exempel Finlands säkerhets- och försvarspolitik, Finlands militära beredskap och utvecklingen av försvaret av landet, den militära prestandan, samhällets kriställighet, försörjningsberedskapen samt forskningen och produktutvecklingen i anknytning till försvaret av landet.

Genom militär underrättelseinhämtning strävar man efter att upptäcka och identifiera personer som avslöjar uppgifter, som med tanke på försvaret av landet ska hållas hemliga för en utländsk underrättelsetjänst, och personer som en sådan tjänst försöker rekrytera. Underrättelseinhämtningen kan hänföra sig även till en underrättelsetjänsts öppna och hemliga underrättelseinhämtning. Även en utländsk underrättelsetjänsts mål och prioriteter för underrättelseinhämtning som gäller Finland samt underrättelseobjektet kan vara föremål för ett underrättelseuppdrag inom militär underrättelseinhämtning.

Enligt 4 § 1 mom. 4 punkten i lagen om militär underrättelseverksamhet kan föremålet för militär underrättelseinhämtning vara en främmande stats utvecklande och spridning av militärmateriel. I allmänhet handlar krigsmateriel om material och teknik som utvecklas för en instans med stora resurser, såsom en stat. Verksamheten enligt punkten behöver inte utgöra något direkt hot för Finland, utan informationen är av betydelse för att upptäcka ändringar som äger rum i Finlands säkerhetsmiljö och för att bilda en militärstrategisk lägesbild. Information enligt punkten kan anses vara rentav nödvändig för Finlands militära försvar och beredskap och den är av betydelse även till exempel för beredskapen och skyddet av den civila befolkningen.

Enligt 4 § 2 mom. i lagen om militär underrättelseverksamhet är föremål för den militära underrättelseinhämtningen verksamhet som allvarligt hotar det finska försvaret. Med det finska försvaret avses den helhet av försvaret som tryggar den territoriella integriteten, levnadsmöjligheterna för medborgarna och deras grundläggande fri- och rättigheter, statsledningens verksamhetsfrihet samt den lagliga samhällsordningen. Den verksamhet som utgör målet behöver inte vara av militär natur. Det räcker att verksamheten allvarligt hotar Finlands nationella säkerhet, det vill säga verksamhet vars mål är att orsaka störningar och förlama funktioner som är viktiga för försvaret av landet, såsom ledningen, logistiken och datatrafiken.

Ett informationsintresse kan anses i det första rummet anknyta till vilken instans som orsakar ett sådant hot och vad som förklarar hot, det vill säga vad som är avsikten med hotet. Det kan handla om sabotage eller bemanning av ett område genom att använda proxyaktörer för en fientligt sinnad stat. Underrättelseinhämtning enligt punkten kan riktas på ett aktörsneutralt sätt.

Ett hot mot det finska försvaret kan avsevärt påverka Finlands utrikespolitiska ställning och reducera dess politiska svängrum. Det kan anses att de allvarskriterium som gäller hotet uppfylls även i situationer som kan utveckla sig till kränkningar av den territoriella integriteten eller som äventyrar de grundläggande elementen för samhällsfreden, såsom befolkningens psykiska kristolerans och funktionsförmåga.

Underrättelseinhämtning enligt punkten täcker de vitala samhällsfunktionerna (ledning, internationell verksamhet, EU-verksamhet, försvarsförmågan, den inre säkerheten, ekonomin,

infrastrukturen och försörjningsberedskapen, befolkningens funktionsförmåga samt den psykiska uthålligheten). Det kan anses att funktionerna är sammanflätade med konstitutionella ”superintressen”. Det handlar om de intressen som ska tryggas i enlighet med de uppgifter som föreskrivits för Försvarsmakten.

Det är möjligt att man försöker påverka de vitala samhällsfunktionerna med ett stort antal olika metoder, såsom i tilltagande grad med cyberpåverkan.

Ovan konstaterade föremål för militär underrättelseinhämtning kan anses höra endast till militär underrättelseinhämtning. Dessutom finns det även föremål som är gemensamma för den militära underrättelseinhämtningen och skyddspoliserna. Den underrättelseinhämtning som gäller föremålen koordineras mellan underrättelsemyndigheterna och genom till exempel de prioriteter i underrättelseinhämtningen vilka anvisats på statsrådsnivå.

Enligt 4 § 1 mom. 3 punkten i lagen om militär underrättelseverksamhet är föremål för militär underrättelseverksamhet planering, tillverkning, spridning och användning av massförstörelsevapen. Det handlar för egen del om proliferationsövervakning, som avser att förhindra att massförstörelsevapen och bärare för sådana förhindras samt att anordningar, redskap, material, kunskap och färdigheter som används för att tillverka massförstörelsevapen sprids till aktörer som strävar efter att utveckla ett massförstörelsevapen.

Inhämtande av information i militär underrättelseinhämtning hänför sig framför allt till massförstörelsevapen hos en statlig aktör och en jämförbar aktör. Till exempel nervgiftet Novitjok som användes i Sergei Skripal-fallet är ett kemiskt vapen som tydligt utvecklats för militär verksamhet och som även användes av en fientlig sinnad stats militära underrättelsetjänst. Vid civil underrättelseinhämtning ligger betoningen till exempel på terroristiska aktörer.

Enligt 4 § 1 mom. 5 punkten i lagen om militär underrättelseverksamhet är föremål för militär underrättelseverksamhet en kris som allvarligt hotar internationell fred och säkerhet. En kris enligt punkten är alltid en kris som är större än ett internt nödläge i en enskild stat, det vill säga att kriserna har konsekvenser även för statens grannländer. Information kan inhämtas om utvecklingen för den politiska situationen i den stat som står i centrum eller i anknutna stater samt om de eventuella utrikes- och säkerhetspolitiska följderna av ärendet för Finland. Ett hot mot den internationella freden och säkerheten kan uppkomma även via epidemier och pandemier.

Huruvida det handlar om en kris som allvarligt hotar den internationella freden eller säkerheten kan definieras genom att exempelvis utgå från att ett möte för republikens president och utrikes- och säkerhetspolitiska ministerutskottet sammankallas med anledning av ärendet.

Enligt 4 § 1 mom. 6 punkten i lagen om militär underrättelseverksamhet är föremål för militär underrättelseverksamhet verksamhet som allvarligt hotar säkerheten vid internationella krishanteringsinsatser. Finland deltar i den internationella militära krishanteringen, vars syfte är att bevara och återställa den internationella freden och säkerheten eller att stödja humanitär biståndsverksamhet eller skydda civilbefolkningen.

Syftet med inhämtande av information är att säkerställa operationssäkerheten och den personliga integriteten för den personal som deltar i den. Information kan skaffas till exempel om förhållandena i ett område för en krishanteringsoperation och om möjligheten för att personalen är föremål för en våldsam attack. Inhämtandet av information kan även göras på ett

föregripande sätt, vilket är av betydelse med tanke på beslutsfattandet om deltagandet i operationen.

Enligt 4 § 1 mom. 7 punkten i lagen om militär underrättelseverksamhet är föremål för militär underrättelseverksamhet verksamhet som allvarligt hotar säkerheten i samband med att Finland ger internationellt bistånd. Punkten omfattar även verksamhet enligt EU:s solidaritetsklausul.

I till exempel verkställighetssituationer enligt solidaritetsklausulen, det vill säga i situationer som kan handla om en storolycka som orsakas av naturen eller mänsklig aktivitet, är det ofta nödvändigt att få information om förhållandena i det område som drabbats av en attack eller olycka. Det samma gäller även för situationer med ömsesidigt bistånd, såsom ett beslut att skicka Europeiska unionens stridsgrupper eller Natos snabbinsatsstyrka till en militär operation eller en grupp av finländska experter till specialuppdrag i utlandet. Det fastställda objektet lämpar sig för inhämtande av information för att få en uppfattning om de färdigheter som behövs i operationen och förhållandena på genomförandeplatsen, men även om de omständigheter som påverkar säkerheten för den personal som sänts via den mekanism som valts i respektive fall.

Även situationer som är gemensamma för militär och civil underrättelseinhämtning täcks av 4 § 2 mom. i lagen om militär underrättelseverksamhet. I fråga om militär underrättelseinhämtning har föremålet behandlats tidigare.

2.2.1.2 Mekanismerna för att begränsa underrättelseverksamhet

Allmänt

Underrättelseverksamhet som baserar sig på hot kan anses rikta sig mot ett obegränsat antal människor. Därför innehåller lagen bestämmelser om olika styrnings-, avgränsnings- och begränsningsmekanismer. Avgränsningarna är tydligast exempelvis i fråga om de allmänna och särskilda förutsättningarna för metoderna för underrättelseinhämtning, som antingen är tillämpliga eller inte tillämpliga.

Lagen innehåller även bestämmelser om principerna för militär underrättelseverksamhet, vilka är flexibla än för användningen av en metod för underrättelseinhämtning och täcker olika situationer. Principen styr snarare än begränsar underrättelseverksamheten och det anknutna beslutsfattandet. Principerna kan ses som optimeringsorder med vilka man uppnår ett värde eller ett mål i så hög grad som de juridiska och faktiska randvillkoren möjliggör det. I fråga om lagstiftningen om militär underrättelseverksamhet kan principerna anses belysa värdegrunden för underrättelseverksamheten. Via principerna får beslutsfattandet om militär underrättelseverksamhet lösningsgrunder som utvecklas till exempel i tolkningspraxis för grundlagen och de människorättskonventioner som binder Finland. Principerna framkommer framför allt i samband med bestämmelserna med utrymme för prövningsrätt, vilket betonas i militär underrättelseverksamhet.

Grundlagsutskottet har betonat att skyldigheten att påvisa en underrättelseåtgärds överensstämmelse med de allmänna principer som tillämpas på underrättelseverksamhet i varje enskilda fall alltid ligger hos underrättelsemyndigheten, som även i övrigt har en skyldighet lägga fram motiveringar som visar att de lagstadgade förutsättningarna för en underrättelseåtgärd är uppfyllda (GrUU 35/2018 rd, s. 16 och GrUU 36/2018 rd, s. 18).

Utöver de principer som allmänt styr verksamheten innehåller lagen bestämmelser om minimeringsmekanismer, vars mål att filtrera information som inhämtats av en militärunderrättelsemyndighet till vad som omfattas av militärunderrättelsemyndighetens

befogenhet. Vid militär underrättelseinhämtning är det oundvikligt att man inhämtar information som gäller en utomstående eller som i övrigt är av sådan natur som inte får inhämtas vid militär underrättelseinhämtning. Minimeringsmekanismerna genomförs exempelvis via regleringen kring direktutplåning.

Allmänna principer

Enligt principen om respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna (5 § i lagen om militär underrättelseverksamhet) ska en militärunderrättelsemyndighet respektera de grundläggande fri- och rättigheterna och de mänskliga rättigheterna, och när han eller hon utövar sina befogenheter välja det motiverbara alternativ som bäst tillgodoser dessa rättigheter. De grundläggande fri- och rättigheterna är redan i sig på grundlagsnivå förpliktande för dem som tillämpar lagen. Även om de grundläggande fri- och rättigheterna ska tillgodoses redan som en direkt tillämplig rättighet, framgår deras betydelse oftast som en tolkningskonsekvens då lagarna tillämpas. Slutresultatet av tolkningen ska stå i samklang med normerna för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. I fråga om lagstiftningen om militär underrättelseinhämtning har grundlagsutskottets i sin utlåtandepraxis (GrUU 36/2018 rd, s. 15) konstaterat att dess särdrag förutsätter om att de grundläggande fri- och rättigheterna och de mänskliga rättigheterna iakttas i tolkningen av regleringen om befogenheter inom underrättelseverksamhet.

Enligt proportionalitetsprincipen (6 § i lagen om militär underrättelseverksamhet) ska den militära underrättelseinhämtnings åtgärder vara försvarbara i förhållande till hur viktiga de uppgifter är som erhålls genom informationsinhämtningen, till hur brådskande underrättelseuppgiften är, till det eftersträvade målet för den militära underrättelseinhämtningen, till föremålet för den militära underrättelseinhämtningen, till den inskränkning av rättigheter som andra orsakas av att en underrättelseåtgärd används samt till andra omständigheter som påverkar saken. Åtgärden ska även ge tillräckliga faktiska möjligheter att uppnå de godtagbara mål som ställts upp för den militära underrättelseinhämtningen. Principen syns framför allt i bedömningen av åtgärdernas proportionalitet. De använda metoderna och de olägenheter som orsakats genom dessa, såsom ingripande i skyddet för privatlivet, ska stå i rimlig proportion till det eftersträvade målet. Med detta avses dock inte endast att en överdimensionerad åtgärd förebyggs, utan även att åtgärden är tillräckligt effektiv med tanke på uppnåendet av målet. Proportionalitetsprincipen styr även valet i fråga om de tillgängliga metoderna för underrättelseinhämtning även vad gäller om det är möjligt att inom en kortare tid få den uppgift som behövs genom att använda en annan metod för underrättelseinhämtning – med tanke på skyddet före föremålets integritet kan det vara mer befogat att använda en metod för underrättelseinhämtning som innebär ett djupare ingrepp i skyddet för privatlivet, om den kan användas i en kortare tid (RP 203/2017 rd, s. 200).

Vid tillämpningen av proportionalitetsprincipen kan man beakta även uppdragets vikt: ju allvarigare hot det handlar om och ju större sannolikheten för att hotet blir verklighet bedöms vara, desto försvarligare kan det anses vara att använda metoder för underrättelseinhämtning som innebär en djupare inskränkning av de grundläggande fri- och rättigheterna. På motsvarande sätt kan proportionalitetsprincipen leda till en annan riktning, till exempel om man förmodar att de uppgifter som fås inte är av stor betydelse, och å andra sidan att man genom andra metoder för underrättelseinhämtning gör mindre ingrepp i föremålets rättigheter.

Proportionalitetsprincipens vikt har betonats även i Europadomstolens och EU-domstolens avgörandepraxis. Detta har belysts i synnerhet i de fall som gäller underrättelseinhämtning som avser datatrafik (till exempel *Zakharov mot Ryssland*, *Weber och Saravia mot Tyskland* och *Digital Rights C-293/12*). Proportionalitet betonas framför allt av att man på grund av

konsekvenserna för utomstående kräver att underrättelseinhämtning som avser datatrafik ska vara den metod som tillgrips i sista hand.

Den sista meningen i 6 § i lagen om militär underrättelseverksamhet, vilken gäller kravet på att åtgärdernas faktiska lämplighet för deras ändamål ger uttryck för grundlagsutskottets riktlinje om att en begränsning av de grundläggande fri- och rättigheterna inte kan lämpa sig för dess syfte och således vara nödvändig, om man med den inte ens i princip kan uppnå det godtagbara mål som ligger till grund för den (GrUU 36/2018 rd, s. 17 och till exempel GrUU 40/2017 rd, s. 4, GrUU 55/2016 rd, s. 4-5 och GrUU 5/2009 rd, s. 3). I praktiken framgår detta av att en militärunderrättelsemyndighet ska lägga fram en tillräcklig motivering om lämpligheten för metoden för underrättelseinhämtning för dess ändamål till den domstol eller en annan beslutsfattare som avgör tillståndsärendet (FsUB 9/2018 rd, s. 31)

Principen om minsta olägenhet (7 § i lagen om militär underrättelseverksamhet) styr en militärunderrättelsemyndighets befogenhetsanvändning på så sätt att det genom användning av den inte får ingripas i någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenhet än vad som är nödvändigt för att utföra uppdraget. Dessutom innehåller principen om minsta olägenhet ett krav enligt vilket man genom inhämtande av information inte får ingripa i hemligheten i fråga om förtroliga meddelanden på ett annat än på ett så riktat och begränsat sätt som möjligt (LaUU 31/2018 rd, s. 3-4 och GrUU 36/2018 rd, s. 17). I tillämpningen av principen ska man utöver det egentliga föremålet för underrättelseinhämtningen beakta även utomstående, eftersom uttryckligen ”inte någon” nämns i bestämmelsen. Rättigheter kan anses avse framför allt de grundläggande fri- och rättigheter som föreskrivits i grundlagen (RP 202/2017 rd, s. 179).

Myndighetsorganisationer från främmande stater åtnjuter inte något skydd för de grundläggande fri- och rättigheterna, varför det är möjligt att rikta mer signifikativa underrättelseåtgärder mot dessa jämfört med icke-statliga föremål (privatpersoner). Olägenheten är alltså minst då underrättelseinhämtningen hänför sig till kommunikationen av en främmande stats myndighet, även om det kan krävas att man gör ingrepp i skyddet för hemligheten i fråga om förtroliga meddelanden för att upptäcka sådan.

I praktiken styr principen till att använda den metod för underrättelseinhämtning som orsakar den minsta skadan eller olägenheten för föremålet. Med andra ord ska man bland metoderna för underrättelseinhämtning välja den som allra minst inskränker i målpersonens grundläggande fri- och rättigheter och mänskliga rättigheter. Med tanke på tillämpningen av principen ska man i fråga om föremålen beakta om det handlar om en statlig aktör eller en icke-statlig aktör på grund av att skyddet för de grundläggande fri- och rättigheterna är olika för dessa. Å andra sidan styr principen till att välja den metod för underrättelseinhämtning som kan riktas på bästa sätt. Den exakta inriktningen avgränsar den skada eller olägenhet som den orsakar för utomstående. En militärunderrättelsemyndighet ska bedöma olägenhetens grad vid föremålet, men även antalet utomstående som eventuellt omfattas av olägenheten.

För att minimera en olägenhet för utomstående förutsätter principen om minsta olägenhet att man väljer den metod för underrättelseinhämtning som kan riktas på det noggrannaste sättet. Bedömningen av den minsta olägenheten sker på övergripande sätt och som en fallspecifik vägning, där den eftersträlvade nyttan och nödvändigheten att inskränka en individs rättigheter för att uppnå målet står mot varandra.

Grundlagsutskottet har i sitt betänkande (GrUB 4/2018 rd, s. 7–8) ansett att det för att uppfylla nödvändighetskravet inte är tillräckligt att inhämtande av information som hänför sig till förtroliga meddelanden anses allmänt främja försvaret av landet eller den nationella säkerheten,

utan man ska kunna visa att man genom att använda metoden för underrättelseinhämtning på befogade grunder kan anta att man får information om verksamhet som orsakar ett hot för försvaret av landet eller den nationella säkerheten. I tillämpningen av principen ska man bedöma nödvändigheten av att göra inskränkningar med tanke på uppgiften.

Enligt principen om ändamålsbundenhet får en militärunderrättelsemyndighet använda en befogenhet endast för de syften som anges i denna lag (8 § i lagen om militär underrättelseverksamhet). Bestämmelsen kan anses vara informativ i den mån att en myndighet redan med stöd av grundlagen ska förfara enligt lagen. Principen påminner att användningen av befogenheten ska basera sig på en uttrycklig bestämmelse och det syfte som ställts i detta, men å andra sidan kan principen anses omfatta ett förbud mot missbruk, det vill säga att befogenheter får användas endast inom de gränser som det föreskrivna syftet och målen ställer.

Förbudet med diskriminering (9 § i lagen om militär underrättelseverksamhet) uttrycker det förbud som redan föreskrivits i 6 § 2 mom. i grundlagen, enligt vilket alla former av diskriminering är förbjuden. Bestämmelsen kan dock anses vara betydelsefull som ett uttryck för förbudet mot profilering i militär underrättelseverksamhet. Framför allt kan profilering anses vara problematiskt med tanke på skyddet för privatlivet och personuppgifter samt de grundläggande fri- och rättigheter som gäller jämlikhet. I praktiken kan det även anses att profilering är ineffektiv, eftersom den ofta hänför sig till ett onödigt stort antal människor och å andra sidan kan den även lämna potentiella målpersoner utanför gallringen. I fråga om målen med diskrimineringsförbudet kan den anses delvis överlappa de andra principerna.

I synnerhet i fråga om internationellt samarbete kan man även tala om en oreglerad förtroendepincip för informationsutbytet. I rättslitteraturen har man ansett att den baserar sig på kravet på ömsesidigt förtroende mellan parterna, vilket i praktiken förutsätts i internationellt informationsutbyte. Uppgifter som fås genom verksamheten får användas endast för det ändamål för vilket de getts, och uppgifterna får inte överlåtas vidare utan uttryckligt samtycke av den som lämnat uppgifterna. Parterna i informationsutbytet litar på att dessa villkor iaktas oberoende av om den utlämnade handlingen innehåller en separat sekretessmärkning eller en klausul om ett utlämnandeförbud (se även HD:2010:31).

Principen kan anses handla om en norm som etablerats i den internationella sedvanerätten, för vilken vägande praktiska orsaker ska läggas fram. Genom att iaktta principen tryggas pågående operationer, den personliga integriteten för informationskällor eller andra som på annat sätt deltar i dessa samt de internationella relationerna. En part som förlorar detta förtroende i det internationella säkerhets- och underrättelsetjänstssamarbetet lämnar utanför informationsutbytet, fram till dess att förtroendet har byggts upp på nytt. Med tanke på underrättelsemyndigheten är iakttagande av förtroendepincipen i informationsutbyte en hörnsten i förutsättningarna för dess verksamhetsförutsättningar.

Vid militär underrättelseverksamhet är det även möjligt att utöver ovan konstaterade principer identifiera en betydande styrande omständighet – operationssäkerheten. Den centrala förutsättningen för militär underrättelseverksamhet är att man agerar i hemlighet för föremålet. Det centrala elementet i all militär underrättelseverksamhet är huruvida åtgärden och i bredare omfattningen även verksamheten kan hållas hemlig. Detta påverkar planeringen av den operativa verksamheten på alla nivåer, även på tillämpningen av lagen. Om en åtgärd leder till att den militära underrättelseverksamheten avslöjas, även om den avslöjas endast partiellt, eller om risken för att den avslöjas anses vara för stor, ska åtgärden inte vidtas.

Minimeringsmekanismerna

De allmänna principerna skapar och redogör för värdegrunden för militär underrättelseinhämtning och styr till att använda rätt metod för underrättelseinhämtning, medan minimeringsmekanismerna strävar efter att avgränsa information som i sig fåtts med en rätt och korrekt använd metod för underrättelseinhämtning till vad som avsetts med användningen av den. Genom avgränsningen strävar man efter att begränsa inskränkningen i skyddet för privatlivet efter att förutsättningarna för metoden för underrättelseinhämtning har uppfyllts och den egentliga användningen av den börjar. Detta har även en viktig betydelse för en individs rättsskydd. Minimeringsmekanismerna kan anses omfatta underrättelseförbud, granskning av upptagningar och dokument, undersökning av upptagningar, användning av överskottsinformation, utplåning av uppgifter och bestämmelserna om avbrytande av metoder för underrättelseinhämtning samt bestämmelserna om utnyttjandeförbud.

Minimeringsmekanismerna är även av betydelse med tanke på regleringens förutsägbarhet, eftersom de avgränsar den militära underrättelseinhämtningen på så sätt att metoder för militär underrättelseinhämtning riktas endast mot uppgifter som är av betydelse för objektet för den militära underrättelseinhämtningen, genom att undvika att en metod för militär underrättelseinhämtning som riktar sig mot utomstående används. Således kan en individ inte förutse situationer där han eller hon kan bli föremål för användning av en metod för underrättelseinhämtning.

I synnerhet i militär underrättelseverksamhet har minimeringsmekanismerna en särskild betydelse då föremålen för den militära underrättelseverksamheten ligger på fenomennivå och användningen av metoder för underrättelseinhämtning således kan tillämpas på ett jämförelsevis omfattande sätt. Således är det även möjligt att myndigheten utövar prövningsrätt och misstar sig. Genom minimeringsmekanismerna begränsas att man på obefogade grunder gör inskränkningar av skyddet för privatlivet, vilket kan framgå tydligare i situationer där förutsättningarna för användning av en metod för underrättelseinhämtning i sig är uppfyllda, men man vid användningen av en metod för underrättelseinhämtning upptäcker att sakläget är ett helt annat.

Det finns bestämmelser som motsvarar bestämmelserna om underrättelseförbud i 82 och 83 § i lagen om militär underrättelseverksamhet i 17 kap. (571/1948) i rättegångsbalken (4/1734) och i beslags- och kopieringsförbuden enligt 7 kap. 3 § i tvångsmedelslagen. Skillnaden till avlyssnings- och observationsförbuden i anknytning till brott är dock att syftet med militär underrättelseinhämtning inte är att verkställa straffansvaret. Syftet med avlyssnings- och observationsförbuden är således att förbjuda användning av information i strid med rättsstatliga grunder och skydda hemligheten i fråga om ett förtroligt meddelande och människornas privatliv.

Man kan dock anse att de viktigaste förbudet mot underrättelseinhämtning utgörs av förbudet mot underrättelseinhämtning som avser datatrafik – vid underrättelseinhämtning som avser datatrafik är det inte fullt ut möjligt att förvissa sig om att den datatrafik som inkommer till systemet på riktigt och avsiktligt är trafik som har en natur av trafik som passerar Finlands gräns. Således är det oundvikligt att även datatrafik som avsetts att vara intern trafik i Finland når systemet. Utifrån underrättelseförbudet ska datatrafik utplånas om avsändaren och mottagaren finns i Finland. Även de motsvarande förbud som föreskrivs i 82 och 83 § i lagen gäller för underrättelseinhämtning som avser datatrafik.

Enligt bestämmelserna om utplåning ska underrättelser utplånas utan dröjsmål efter att det kommit fram att uppgifterna inte behövs för att sköta uppdrag inom militär underrättelseinhämtning eller för försvaret av landet eller för att trygga den nationella säkerheten. Det handlar om en allmän skyldighet att utplåna underrättelser, vilken gäller för alla

metoder för underrättelseinhämtning och all information som fåtts genom dem. Utplåningsskyldigheten ska fullgöras direkt då det framgår att en uppgift inte är betydelsefull.

På motsvarande sätt omfattar skyldigheten att utplåna uppgifter även uppgifter som fåtts genom användning av en metod för underrättelseinhämtning vilken beslutats i en akut situation, där beslutet av den som fattat beslutet om den brådskande användningen av en metod för underrättelseinhämtning inte är giltigt i det egentliga beslutfattandet. I dessa situationer ska den information som fåtts genom användningen av metoden för underrättelseinhämtningen utplånas omedelbart.

Bestämmelserna om granskning av upptagningar och handlingar och undersökning av upptagningar garanterar för egen del en individs rättsskydd genom att begränsa ingreppet i skyddet för privatlivet. Genom granskningen och utplåningen av uppgifter är det möjligt att få visshet om att endast behöriga uppgifter används och att till exempel uppgifter om utomstående utplånas. Genom granskningen och utplåningen av uppgifter är det möjligt att få visshet om att endast behöriga uppgifter används och att till exempel uppgifter om utomstående utplånas. Bestämmelserna garanterar för egen del en individs rättsskydd genom att begränsa ingreppet i skyddet för privatlivet.

Det finns bestämmelser om avbrytande av användningen av en metod för underrättelseinhämtning i 85 § i lagen om militär underrättelseverksamhet. I 1 mom. i paragrafen föreskrivs att om det kommer fram att teleavlyssningen eller teleövervakningen riktas mot något annat än i tillståndet avsett meddelande från eller till den person som är föremål för tillståndet eller att den person som är föremål för den tekniska avlyssningen riktas mot inte befinner sig i det utrymme eller på den plats som avlyssnas, ska användningen av metoden för underrättelseinhämtning avbrytas så snart som möjligt, och de upptagningar som har fåtts genom avlyssningen och anteckningarna om de uppgifter som fåtts genom den ska genast utplånas.

På motsvarande sätt innehåller paragrafens 2 och 3 mom. bestämmelser om avbrytande av radiosignalspaning och teknisk observation av utrustning.

I fråga om underrättelseinhämtning som avser datatrafik regleras avbrytandet genom att i 86 § 1 mom. hänvisa till 82 § 2 mom. i lagen. Om det under underrättelseinhämtning som avser datatrafik eller i övrigt kommer fram att det handlar om ett meddelande som inte får avlyssnas eller observeras, ska åtgärden således avbrytas och de upptagningar som fåtts genom den och anteckningarna om de uppgifter som fåtts genom den utplånas utan dröjsmål. Om ett sökbegrepp som använts i underrättelseinhämtning som avser datatrafik hänför sig till fel objekt eller till datatrafik som den inte får hänföra sig till, ska användningen av sökbegreppet med andra ord avslutas och de uppgifter som fåtts med det utplånas.

Sammanfattningsvis kan man konstatera att minimeringsmekanismerna för egen del garanterar rättsskyddet för en individ och förebygger godtycklighet av myndigheterna. Som helhet kan det bedömas att man i Finland utfärdat omfattande bestämmelser om minimeringsmekanismerna. Lagstiftningen innehåller bestämmelser till exempel om granskning av upptagningar och handlingar, undersökning av upptagningar samt utplåning av uppgifter. Dessutom finns det bestämmelser om underrättelseförbud. Regleringen kring minimeringsmekanismer verkar allmänt taget även motsvara kraven i Europakonventionen väl.

Tillgodoseendet av proportionalitet och förutsebarhet garanteras av ett militärunderrättelsemyndigheten har en skyldighet att utplåna uppgifter som omfattas av underrättelseförbuden och utplåningsskyldigheten. Förfarandet kan för egen del anses vara

tillräckligt för att trygga att en individs rättsskydd och principerna om en rättsstat tillgodoses. Tillgodoseendet av underrättelseförbud och utplåningsskyldigheterna övervakas av en myndighetsextern instans, underrättelsetillsynsombudsmannen.

2.2.2 Utlämnande av information om sabotageprogram

I 18 § i lagen om militär underrättelseverksamhet finns det bestämmelser om samarbete med andra myndigheter och med företag och andra sammanslutningar. Enligt dess 2 mom. kan militärunderrättelsemyndigheterna för att genomföra sitt uppdrag trots sekretessbestämmelserna till företag och andra sammanslutningar lämna ut identifieringsuppgifter som anknyter till sabotageprogram och som behövs för utvecklingen av metoder och system för underrättelseinhämtning eller lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är nödvändigt med avseende på Forsvarsmaktens verksamhet eller för att skydda den nationella säkerheten.

Dessutom kan uppgifter om ett skadligt datorprogram lämnas ut med stöd av 74 § i lagen, om uppgiften inhämtats genom att använda med hjälp av underrättelseinhämtning som avser datatrafik.

2.2.3 Installation och avinstallation av anordningar, metoder eller programvaror

Enligt 42 § i lagen om militär underrättelseverksamhet har en tjänsteman som är anställd vid 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 vid en militärunderrättelsemyndighet då rätt att i hemlighet ta sig in i ovannämnda 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 får inte installeras eller avinstalleras i utrymmen som används för boende av permanent natur.

Enligt förarbetena till lagen (RP 203/2017 rd, s. 262) handlar bestämmelsen framför allt om en åtgärd som främjar metoder av observationstyp, med vilken man i praktiken möjliggör en effektiv användning av den aktuella befogenheten. I praktiken fås ett tillstånd till installation och avinstallation i beslut om användning av en befogenhet eller i samband med att ett tillstånd beviljas.

På det sätt som konstaterats i förarbetena till lagen (RP 203/2017 rd, s. 261–262) har den som tillämpar lagen getts utrymme för prövning beträffande när man vidtar en åtgärd och när användningen av en åtgärd avslutas. För att förhindra att användningen av en metod för underrättelseinhämtning avslöjas har detta ansetts vara nödvändigt. När åtgärden vidtas ska man därtill fundera på den eventuella risken för att åka fast och risken för att en skada orsakas för objektet av åtgärden. Genom militärunderrättelsemyndighetens åtgärder är det således inte tillåtet att orsaka någon större skada eller olägenhet än vad som är nödvändigt i samband med att en anordning, metod eller programvara installeras och avinstalleras. Installation och avinstallation ska hålla åtskilt från användningen av den egentliga metoden för underrättelseinhämtning, som är föremål för ett separat beslut om inledande eller avslutande av metoden.

2.2.4 Underrättelseinhämtning som avser datasystem i Finland

Lagen om militär underrättelseverksamhet ger en möjlighet för en militärunderrättelsemyndighet att inhämta information som gäller elektroniska kommunikations- och informationsbehandlingsinstrument och kommunikation mellan dessa genom att utöva befogenheterna till teleavlyssning (34 §), teleövervakning (37 §), teknisk avlyssning (26 §) och teknisk observation av utrustning (32 §) samt befogenheter till stöd för dessa, såsom installation av en anordning, metod eller programvara som används för ovan nämnda metoder för underrättelseinhämtning bland annat i datasystem (42 §). På grund av den kasuistiska regleringen kring metoder som ingriper i skyddet för hemligheten i fråga om förtroliga meddelanden måste man så gott som utan undantag använda de ovan nämnda metoderna parallellt med varandra då information inhämtas om samma hot, till exempel om en främmande stats cyberhotverksamhet. Även om det är nödvändigt att samtidigt använda flera metoder för att inhämta tillräcklig information, kan ett hinder för den parallella användningen av dessa orsakas av att riktandet av de olika metoderna har fastställts på ett sätt som avviker från varandra.

Enligt 34 § 1 mom. i lagen om militär underrättelseverksamhet avses med teleavlyssning att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett i 3 § 43 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) avsett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät eller någon annan kommunikationsförbindelse avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och identifieringsuppgifterna i anslutning till det.

Enligt 36 § 3 mom. i lagen om militär underrättelseverksamhet ska man i ett yrkande och i ett beslut om teleavlyssning nämna den person, teleadress eller teleterminalutrustning som åtgärden riktas mot.

Enligt 37 § 1 mom. i lagen om militär underrättelseverksamhet 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 lokaliseringsuppgifter om en teleadress eller teleterminalutrustning inhämtas.

Enligt 38 § 3 mom. i lagen om militär underrättelseverksamhet ska man i ett yrkande och i ett beslut om teleövervakning på ett sätt som motsvarar ett yrkande och ett beslut om teleavlyssning nämna den person, teleadress eller teleterminalutrustning som åtgärden riktas mot.

Enligt 32 § 1 mom. i lagen om militär underrättelseverksamhet avses med teknisk observation av utrustning 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.

Enligt 33 § 3 mom. i lagen om militär underrättelseverksamhet ska man i ett yrkande och i ett beslut om teknisk observation av utrustning nämna den tekniska anordning eller programvara som åtgärden riktas mot.

Enligt 26 § 1 mom. i lagen om militär underrättelseverksamhet avses med teknisk avlyssning att en persons eller, i det fall att en bestämd person inte kan specificeras, persongrups 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 verksamhet som bedrivs av en i 4 mom. i avsedd person.

Enligt 27 § 4 mom. i lagen om militär underrättelseverksamhet ska man i ett yrkande och i ett beslut om teknisk avlyssning nämna den person eller, i det fall att en bestämd person inte kan specificeras, grupp av personer, tillräckligt specificerad, eller det utrymme eller den plats av annat slag som åtgärden riktas mot.

Befogenheten till teknisk avlyssning kan karakteriseras som en allmän befogenhet som gör det möjligt att inhämta information som gäller kommunikation som bedrivs av en person som åtnjuter skyddet för förtroliga meddelanden. Tillämpningsområdet för teknisk avlyssning har inte direkt avgränsats i definitionsbestämmelsen av denna befogenhet. Däremot har dess tillämpningsområde reducerats genom att utfärda separata bestämmelser om teleavlyssning, teleövervakning och teknisk observation av utrustning samt definitionerna av dessa. Bestämmelserna med definitioner av teleavlyssning och teleövervakning redogör för att dessa befogenheter tillämpas då inhämtandet av information hänför sig till ett meddelande som förmedlas i ett allmänt kommunikationsnät eller i ett kommunikationsnät som anslutits till det. Det ser ut som om det varit nödvändigt att avskilja teleavlyssning och teleövervakning från området för teknisk avlyssning i huvudsak därför att dessa metoder, med avvikelse från det övriga inhämtandet av information som hänför sig till kommunikation, i regel måste genomföras med hjälp av kommunikationsförmedlaren (ett teleföretag), varför det funnits ett behov av att separat utfärda bestämmelser om skyldigheten för en kommunikationsförmedlare att bistå en myndighet i genomförandet av teleavlyssning och -övervakning. I definitionsbestämmelsen av teknisk observation av utrustning föreskrivs att om information om kommunikation eller annan information finns i en teknisk utrustning, tillämpas befogenheten till teknisk observation av utrustning i stället för befogenheten till teknisk avlyssning.

I 32 § 2 mom. i lagen om militär underrättelseverksamhet föreskrivs separat att teknisk observation av utrustning inte får hänföras till ett sådant förtroligt meddelande, som är föremål för separata bestämmelser om teleavlyssning, teleövervakning och annan teknisk observation.

Däremot kan ett yrkande om användning av teknisk observation av utrustning vilket framförs till en domstol och ett domstolsbeslut inte gälla en person, utan de gäller med stöd av den nuvarande regleringen alltid en enskild anordning eller en programvara som ingår i en anordning.

I 62 § i lagen om militär underrättelseverksamhet finns det bestämmelser om underrättelseinhämtning som avser utländska datasystem. Enligt paragrafens 1 mom. avses med underrättelseinhämtning som avser utländska datasystem att information inhämtas med datatekniska metoder från ett datasystem utanför Finland. Försvarmaktens underrättelsetjänst får rikta underrättelseinhämtning som avser utländska datasystem på ett datasystem, om detta kan antas vara av synnerlig vikt för att inhämta information med avseende på underrättelseuppdraget.

2.2.5 Teknisk observation av utrustning

Enligt 32 § 1 mom. i lagen om militär underrättelseverksamhet avses med teknisk observation av utrustning 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 sinnesförmålor observeras, upptas eller behandlas på något annat sätt för att utreda omständigheter som är behövliga med avseende på ett underrättelseuppdrag.

Enligt 2 mom. i paragrafen får genom teknisk observation av utrustning inte inhämtas information om innehållet i ett meddelande som förmedlas och som avses i 34 § och inte heller om identifieringsuppgifter om ett sådant meddelande.

Enligt paragrafens 3 mom. kan militärunderrättelsemyndigheterna ges tillstånd till teknisk observation av utrustning hos en statlig aktör för utförande av ett underrättelseuppdrag.

Enligt paragrafens 4 mom. kan militärunderrättelsemyndigheterna 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.

Det finns bestämmelser om beslut om teknisk observation av utrustning i 33 § i lagen om militär underrättelseverksamhet. Enligt dess 1 mom. ska beslut om teknisk observation av utrustning 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.

Enligt paragrafens 2 mom. får tillstånd beviljas för högst sex månader åt gången.

Enligt paragrafens 3 mom. ska 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 och 6) eventuella begränsningar och villkor för den tekniska observationen av utrustning.

2.2.6 Underrättelseinhämtning som avser datatrafik

2.2.6.1 Behandling av tekniska data om datatrafik

Det finns bestämmelser om behandling av tekniska data i 66 § i lagen om militär underrättelseverksamhet. Enligt dess 1 mom. får Försvarmaktens underrättelsetjänst för inriktning av underrättelseinhämtning som avser datatrafik 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.

Enligt paragrafens 2 mom. får i resultatet av den statistiska analysen inte ingå sådan information genom vilken en enskild fysisk person kan identifieras.

Enligt paragrafens 3 mom. ska Försvarmaktens underrättelsetjänst förstöra insamlade och lagrade tekniska data om datatrafiken omedelbart efter det att resultatet av den statistiska analysen har blivit klart.

2.2.6.2 Sökbegreppen i underrättelseinhämtning som avser datatrafik

Enligt 10 § 1 mom. 1 punkten i lagen om militär underrättelseverksamhet avses med sökbegrepp en uppgift som används för att vid underrättelseinhämtning som avser datatrafik så avgränsat och exakt som möjligt i en del av kommunikationsnätet selektera den datatrafik som är föremål för underrättelseinhämtningen, varvid intrånget i skyddet för hemligheten för förtroliga meddelanden sker endast i den omfattning som är nödvändig för att uppnå syftet med underrättelseinhämtningen. Definitionen har utarbetats med riksdagens medverkan (GrUU 9/2018 rd, GrUU 36/2018 rd och GrUU 76/2018 rd).

Enligt 68 § 3 mom. och 70 § 2 mom. i lagen om militär underrättelseverksamhet får som sökbegrepp inte användas uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland.

I förarbetena till lagen (RP 203/2017 rd, s. 297) motiveras bestämmelsen med att om innehavaren av en teleterminalutrustning eller teleadress befinner sig i Finland och identifieringsuppgifterna om denna teleterminalutrustning eller teleadress är kända av en militärunderrättelsemyndighet, ska inhämtandet av information göras med hjälp av de andra metoder för underrättelseinhämtning som föreskrivs i 4 kap. i lagen, såsom teleavlyssning, inhämtande av information i stället för teleavlyssning eller teleövervakning, till den del som de föreskrivna förutsättningarna för dessa uppfylls. Enligt regeringens proposition strävar man på detta sätta att minimera konsekvensen för utomståendes datatrafik.

Enligt 70 § 3 mom. i lagen får underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer inte inriktas utgående från ett meddelandes innehåll, om det inte vid inriktningen används information som beskriver innehållet i ett sabotageprogram. I andra fall är det med andra ord förbjudet att använda sökbegrepp som gäller innehållet i ett meddelande vid automatisk avskiljning av datatrafik.

I förarbetena till lagen (RP 203/2017 rd, s. 149, 291, 297) konstateras att förbudet mot ett så kallat innehållsmässigt sökbegrepp innebär att användning av ett sökbegrepp som beskriver innehållet i ett förtroligt meddelande är helt förbjudet och att man således som sökbegrepp inte får använda uttryck som är en del av det semantiska innehållet i ett förtroligt meddelande eller namn- och identifieringsuppgifter som gäller personer. Enligt förarbetena till lagen handlar det om en avsevärd begränsning som ställts för underrättelseinhämtning, vars syfte är att så långt möjligt trygga kärnområdet i meddelandehemligheten för personer med en ställning som utomstående.

2.2.6.3 Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik

I 86 § i lagen om militär underrättelseverksamhet finns det bestämmelser om utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik. I paragrafens 1 mom. föreskrivs att utöver vad som föreskrivs i 82 § 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 nämns i 82 § 1 mom.

Enligt paragrafens 2 mom. svarar militärunderrättelsemyndigheterna för utplåningen. Om Försvarsmaktens underrättelsetjänst har lämnat uppgifterna till skyddspolisen vid ett tekniskt

genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning, svarar skyddspolisen för utplåningen.

2.2.7 Ingripande i verksamheten i ett informationssystem som äventyrar landets försvar och den nationella säkerheten

2.2.7.1 Den internationella rätten

Den internationella rätten i cybermiljön

Finland har offentliggjort sin syn på den internationella rätten i cybermiljön den 15 oktober 2020. Finland anser att den internationella rätten skapar väsentliga ramar för ansvarsfullt statligt beteende i cybermiljön. Även FN:s mellanstatliga expertgrupp (GGE) har i samma riktning bekräftat att ”den internationella rätten och i synnerhet Förenta nationernas stadga är tillämpliga [i cybersäkerhetsmiljön] och väsentliga omständigheter för att upprätthålla freden och säkerheten och på samma sätt för främjande av en öppen, säker, stabil, nåbar och fredlig informations- och kommunikationsteknologisk miljö”. Den internationella rätten är alltså tillämplig även på cyberverksamhetsmiljön.

Finland anser att *den statliga suveräniteten, det vill säga suveränitetsprincipen*, obestriddligen gäller för cybermiljön. Suveränitet är en primärnorm i den internationella rätten, vars kränkning innebär en gärning i strid med den internationella rätten och ger upphov till statligt ansvar. Denna regel gäller fullt ut även för cybermiljön. Naturen på ett olovligt cyberintrång och följderna av det bestämmer om intrången anses kränka målstatens suveränitet. Det handlar om en fallspecifik bedömning.

Ett stort antal stater anser att varje olovliga intrång i en annan stats datasystem utgör en kränkning av suveräniteten, även om den inte orsakar fysiska skador. Dessutom delar man på brett sätt synen om att suveräniteten kränks i situationer där en cyberoperation orsakar en permanent förlust av funktionsförmågan eller fysiska skador eller personskador.

Även Förenta nationernas generalförsamling har genom flera resolutioner styrkt de frivilliga normer som godkänkts år 2015 av Förenta nationernas mellanstatliga expertgrupp (GGE) och som gäller ansvarsfullt statligt agerande i cybermiljön. Enligt 13 (b) i normen ska staterna inte bedriva eller informationstekniskt sett stödja IKT-verksamhet om avsiktligt skadar kritisk infrastruktur.

Avsiktliga skador på en annan stats datasystem eller hindrande av dess användning kan tolkas som en kränkning av suveräniteten. De situationer där uppgifterna i ett system som utgör objekt endast manipuleras är oklara. Man har ansett att störning av en stats data, datasystem och infrastruktur ska betraktas som en kränkning av suveräniteten, om konsekvenserna inte är ringa.

Fientlig cyberstörning kan även innebära en överträdelse av *förbudet mot att ingripa i en annan stats angelägenheter* under förutsättning att dess syfte är att utöva påtryckningar eller tvång gentemot denna stat i ärenden där den har fri bestämmanderätt (så kallad *domaine réservé*).

I cybermiljön har man ansett att sådana åtgärder omfattar bland annat manipulering av ett valsystem, förlamning av administrativa datasystem och avsiktlig störning av offentlig service. Beroende på naturen av verksamheten kan det även handla om tillämpning av förbudet mot att ingripa i suveräniteten och interna angelägenheter.

En separat fråga utgörs av de så kallade lågintensiva cyberåtgärderna (*low-intensity-cyberåtgärder*), som observerats frekvent under den senaste tiden. Många nuvarande cyberoperationer är lågintensiva åtgärder som inte orsakar fysiska skador. I dessa är det möjligt att man gör intrång i systemen, samlar in information och installerar skadliga programvaror för senare användning. Dessutom orsakar man i stor omfattning mindre olägenheter till exempel för organisationens verksamhet genom att bromsa datasystemens funktion. I varje fall strävar man efter att hålla verksamheten under nivån för en kränkning av den internationella rätten eller åtminstone i sådan form att den inte kan tolkas direkt som en kränkning.

Staterna är oeniga i fråga om huruvida lågintensiva cyberoperationer kränker suveräniteten. En del av staterna anser att gärningar med avsevärda konsekvenser – till exempel operationer som orsakar fysiska skador eller allvarliga operativa störningar – kan kränka suveräniteten. Andra stater anser att alla olovliga intrång i en annan stats datasystem redan i sig är en kränkning av suveräniteten, oberoende av om en konkret skada uppkommer eller ej. Varje stat har en skyldighet att inte tillåta att dess territorium används på ett sätt som orsakar avsevärd olägenhet för andra staters rättigheter. Detta gäller även för cybermiljön. Denna *aktsamhetsplikt (due diligence)* gäller för alla funktioner som omfattar en risk för att orsaka en avsevärd gränsöverskridande olägenhet.

Även om det förekommer oenighet mellan staterna om aktsamhetspliktens förpliktande karaktär, är synpunkten på innehållet i skyldigheten enhetligare. Aktsamhetsplikten är i princip en plikt att agera, inte en plikt som gäller slutresultatet, varför den inte förutsätter att skadliga åtgärder förhindras fullständigt. Den förutsätter dock skäliga åtgärder då en stat känner till eller borde känna till skadliga cyberverksamhet inom dess territorium.

I allmänhet förutsätter rimliga blockeringsåtgärder i cybermiljön att staten vidtar praktiska och tekniskt och politiskt realistiska åtgärder för att förhindra skadliga cyberattacker, om den är medveten om sådana. Skyldigheten att ingripa i skadliga cyberoperationer förutsätter av staten en strävan efter att stoppa eller avgränsa attacker som utgår från dess territorium, även då de görs av en tredje part. Utöver vad som konstaterats ovan har staterna en skyldighet att inte tillåta användning av nät i strid med en annan stats rättigheter.

När en stats cyberoperation kränker dess skyldigheter enligt den internationella rätten, handlar det om en internationellt orättmätig gärning. Reglerna om *tillräknande* i artiklarna om statligt ansvar för FN:s folkrättskommission gäller även i cybermiljön. Om statliga organ eller privata grupper eller privatpersoner som agerar för statens räkning kan identifieras som gärningsmännen i en cyberoperation som kränker en stats internationella plikter, har staten ansvaret för dessa.

För närvarande finns det inte ännu någon etablerad definition av när en cyberattack motsvarar *våld* enligt artikel 2.4 i FN-stadgan eller *väpnat angrepp* enligt artikel 51. Det har dock på omfattande sätt godkänts att överensstämmelsen beror på cyberattackens följder. På motsvarande sätt delar flera andra som kommenterat ärendet åsikten om att en cyberattack som i fråga om omfattning och konsekvenser kan jämföras med ett väpnat angrepp motsvarar ett väpnat angrepp och att man kan besvara det i självförsvar. Maktmedel som tillgrips i självförsvar får dock inte vara oproportionella eller överdimensionerade. Även i cybermiljön ska man iaktta såväl bestämmelserna om maktmedel i FN-stadgan som stadgans syften och mål, som är att förhindra att militär verksamhet eskalerar.

Den *internationella humanitära rätten* är tillämplig på cyberoperationer endast om de är en del av en väpnad konflikt eller sätter igång en väpnad konflikt. Det finns ingen anledning att

bestrida att det skydd som den internationella humanitära rätten erbjuder behövs då man förlitar sig till cybermetoder i pågående väpnade konflikter.

Vid väpnade konflikter ska alla vapen och krigsföringsmetoder användas på så sätt att det är möjligt att iaktta de centrala principerna för internationell humanitär rätt, såsom distinktionsprincipen (*distinction*), proportionalitetsprincipen (*proportionality*) och principen om försiktighetsåtgärder (*precautions*) liksom även den särskilda reglering som baserar sig på dessa principer.

Enligt den internationella humanitära rätten får krigsåtgärder riktas endast mot militära objekt och krigare, inte mot civila och civila mål. Distinktionsprincipen innebär i praktiken att man vid väpnade konflikter inte får rikta åtgärder direkt mot exempelvis civila datorer, elnät eller sjukhusnät. En särskild utmaning utgörs av att i synnerhet data- och elnät ofta används även för militär verksamhet. Enligt den internationella humanitära rätten är militära objekt endast sådana objekt som på grund av deras art, läge, syfte eller användning bildar en viktig del av den militära verksamheten och vars fullständiga eller partiella förstörelse, övertagande eller oskadliggörande innebär en tydlig militär fördel i de förhållanden som råder vid tidpunkten i fråga. Om det förekommer oklarheter om något visst objekt är ett civilt eller militärt objekt, ska objektet anses vara ett civilt objekt.

Enligt proportionalitetsprincipen är ett angrepp förbjudet, om dess förväntade civila skador är för stora i förhållande till den direkta militära nytta som kan uppnås. Denna bedömning kräver dock att en fallspecifik bedömning görs för varje åtgärd. Till exempel om en cyberåtgärd sprider sig från ett militärt kommunikationssystem och på samma gång förlamar datasystemen i en stads sjukhus, är attacken sannolikt oförenlig med proportionalitetsprincipen och olaglig.

I samband med krigsåtgärder ska man kontinuerligt se till att civilbefolkningen och civila mål skonas och parterna i konflikten ska vidta alla tillgängliga försiktighetsåtgärder såväl i samband med attacken som med tanke på attackens konsekvenser för att minimera den skada som orsakas av krigsåtgärderna för civilbefolkningen och civila mål. Detta betonas av att den som vidtar åtgärder bland annat ska använda sådana metoder som kan avgränsas till endast det önskade objektet. I praktiken innebär detta att det inte kan handla om ett sabotageprogram eller en skada som sprids av sig själv.

I bedömningen av vissa cybermetoder kan ge upphov till förbjudna skador, ska även deras synliga direkta och indirekta effekter beaktas. Man ska kontinuerligt sörja för att skyddet av civilbefolkningen och civila mål, inbegripet den väsentliga civila infrastrukturen, service avsedd för civila och civila data (*civilian data*) kan säkerställas.

Dessutom åtnjuter vissa personer och föremål särskilt skydd som omfattas av den internationella humanitära rätten. Sådana är till exempel medicinsk personal och medicinska enheter, såsom sjukhus och deras digitala infrastruktur, humanitär biståndspersonal och objekt som används för humanitära biståndoperationer samt sådana anstalter och konstruktioner som innehåller farlig kraft (dammar, översvämningssvallar, kärnenergidrivna elkraftverk), som om de är föremål för väpnad verksamhet kan orsaka att farliga krafter frigörs och som en följd av det att allvarliga skador orsakas för civilbefolkningen.

Individerna åtnjuter samma *mänskliga rättigheter* och staterna har samma människorättsplikter såväl i nätet som utanför det. Dessutom har varje stat inom sitt territorium och jurisdiktion en plikt att skydda individerna mot kränkningar av dessa rättigheter av andra aktörer.

Åtgärderna mot fientlig cyberverksamhet

Staterna har tillgång till ett stort antal lagliga metoder inom den internationella rätten genom vilka staten kan besvara en kränkning av dess suveränitet.

Retorsion avser ett ovänligt, men helt lagligt svar av en stat på en annan stats föregående verksamhet. Typiska retorsionsåtgärder omfattar exempelvis diplomatiska protester och ekonomiska och kommersiella restriktioner. Retorsion kan användas även då den ursprungliga cyberåtgärden inte entydigt strider mot den internationella rätten. Retorsionsåtgärder i sig innebär inte någon kränkning av den internationella rätten, eftersom de hålls inom ramen för en stats suveräna prövningsrätt.

Motåtgärder är tillåtna endast om den föregående kränkningen av internationell rätt kan räknas till godo för någon stat. På grund av motåtgärdernas exceptionella natur har användningen av sådana begränsats på många sätt. Den mest centrala begränsningen är att motåtgärderna ska vara av temporär natur. Motåtgärden ska även ha ett tidsmässigt samband med rättskränkningen och det är inte möjligt att vidta motåtgärder efter att rättskränkningen upphört. Dessa begränsningar anknyter till att motåtgärder inte kan användas på straffartat sätt, utan deras enda lagliga mål är att få den stat som ansvarar för rättskränkningen att lägga ner sin orättmätiga verksamhet och vid behov ersätta den skada som den orsakat. Motåtgärder omfattas även av proportionalitetskravet: en motåtgärd ska vara av samma mått som rättskränkningens allvar, den aktuella rätten och den lidna skadan. I fråga om motåtgärder finns det procedurregler, enligt vilka en motåtgärd ska meddelas i förväg till den stat som är föremål för en sådan. Det är möjligt att avvika från detta krav, om situationen är så brådskande att den inte ger möjlighet till ett meddelande som ges i förväg. Föreläggningarna har sitt ursprung i de allmänna statsansvarsbestämmelserna i den internationella rätten.

Åtgärder som vidtas utifrån rätten till självförsvar är tillåtna endast om en cyberattack överskrider tröskeln för en väpnad attack och kan tillräknas en viss stat. Enligt artikel 51 i FN-stadgan kan en stat använda självförsvar mot ett väpnat angrepp. Det kan anses att tröskeln överskrids i cybermiljön om cyberåtgärderna orsakar fysiska skador, dödsfall eller skador eller motsvarar sedvanliga väpnade angrepp i fråga om omfattning och konsekvenser (till exempel förstörd infrastruktur). På befogade grunder anses det att en stat som blivit offer för ett sådant angrepp kan besvara det antingen med en nätattack eller med ett väpnat svar. Tillsvidare har inte en enda stat åberopat självförsvarsrätten i fråga om en åtgärd som vidtagits i cybermiljön.

Som ett specialfall kan man nämnda en situation där staten inte själv gjort någon attack, men inte heller hindrat skadlig verksamhet med utgång från dess territorium genom åtgärder som ska anses vara skäliga. I så fall kan staten kränka sin aktsamhetsplikt, vilket kan leda till internationellt ansvar. En stat från vars territorium en cyberattack lanseras har en skyldighet att vidta skäliga åtgärder för att förhindra skadlig cyberverksamhet från dess territorium och förhindra icke-statliga aktörers attacker, om den är medveten om sådana. En försummelse kan även leda till att den kränkta staten vidtar motåtgärder.

Nödvändighetsprincipen (plea of necessity) är en exceptionell grund enligt statsansvarsreglerna, med stöd av vilken en stat tillfälligt kan underlåta att fullgöra sin internationella plikt, om detta är den enda metoden för att skydda sig mot en allvarlig och direkt fara mot ett väsentligt statligt intresse. Tröskeln för att tillämpa tröskeln är synnerligen hög: statliga åtgärder ska vara nödvändiga för att avvärja faran och de får inte allvarligt äventyra andra staters väsentliga intressen. Dessutom kan nödvändigheten inte berättiga åtgärder som överträder normer på ius cogens-nivå eller hot vars uppkomst staten själv bidragit till.

En förutsättning för att åberopa nödvändighet är alltså för det första att faran ska hänföra sig till statens fundamentala intressen, såsom den nationella säkerheten, befolkningens välmående eller

kritiska infrastruktur, som om den rasar kan äventyra statens vitala funktioner. För det andra ska faran vara konkret och snabbt bli verklighet, till exempel ett angrepp med ett mål om att lamslå kritisk infrastruktur. För det tredje är nödvändigheten tillämplig endast om någon annan laglig metod inte är tillgänglig (till exempel diplomati, retorsion eller riktade motåtgärder). För det fjärde får åtgärden inte kränka en annan stats väsentliga intressen.

I en cyberkontext har återopande av nödvändighetsprincipen i princip ansetts vara teoretiskt möjligt, men man har bedömt att det i praktiken är utmanande att tillämpa den, eftersom förutsättningarna för tillämpningen av den sällan skulle uppfyllas. Cybermiljöns särdrag utgörs bland annat av verksamhetens tempo, enkelheten att dölja verksamhetens ursprung och den snabba eskaleringen av skadorna. Nödvändighet kan anses vara en grund som ska tillgripas i sista hand för att tillfälligt underlåta att iaktta en egen plikt i synnerligen exceptionella situationer, varvid det inte finns någon annan metod att tillgripa för att trygga ett vitalt nationellt intresse.

2.2.7.2 Den nationella regleringen

I 1 § i territorialövervakningslagen (755/2000) finns det bestämmelser om lagens tillämpningsområde. Enligt den innehåller lagen i fråga bestämmelser om övervakning och tryggnad av Finlands territoriella integritet. Lagens 23 § innehåller bestämmelser om territorialövervakningsmyndigheterna, vilka enligt paragrafens 1 mom. utgörs av Försvarsmakten, Gränsbevakningsväsendet, polisen, Tullen och dessas tjänstemän som förordnats till territorialövervakningsuppdrag.

I 31 § i lagen finns det bestämmelser om underrättelse om användning av maktmedel. I dess 1 mom. föreskrivs att en territorialövervakningsmyndighet vid utförandet av en i denna lag föreskriven uppgift har rätt att i syfte att bryta motstånd, gripa en person, flytta ett fordon, ett luftfartyg eller ett fartyg eller verkställa ett förordnande enligt 25 § använda sådana behövliga maktmedel som kan anses försvarliga med beaktande av hur viktigt och brådskande uppdraget är, hur farligt motståndet är, de resurser som står till förfogande samt övriga omständigheter som inverkar på helhetsbedömningen av situationen.

I paragrafens 2 mom. föreskrivs att om användningen av maktmedel beslutar den territorialövervakningsmyndighet som utför övervakningen, om inte något annat följer av 33 eller 34 §.

I 33 § i lagen finns det bestämmelser om underrättelse om användning av militära maktmedel. Enligt dess 1 mom. kan Försvarsmakten och gränsbevakningsväsendet för att trygga Finlands territoriella integritet använda behövlig vapenmakt med krigsmateriel som är slagkraftigare än användningen av en militärpersons personliga vapen.

Enligt paragrafens 2 mom. fattas beslut om användning av sådana maktmedel av försvarsministeriet, om inte något annat följer av den behörighet som försvarsmaktens överbefälhavare har eller om något annat inte föreskrivs i 34 §.

I 34 § i lagen finns det bestämmelser om avvärjande av fientlig verksamhet. Enligt dess 1 mom. ska Försvarsmakten och gränsbevakningsväsendet utan dröjsmål vidta alla behövliga åtgärder i syfte att avvärja fientlig verksamhet som medför direkt och allvarlig fara för rikets säkerhet. Då ska vid behov användas sådana i 33 § avsedda maktmedel som kan anses vara försvarliga med beaktande av hur farlig verksamheten är och övriga omständigheter som inverkar på helhetsbedömningen av situationen. Försvarsministeriet ska utan dröjsmål underrättas om att åtgärder vidtas.

I paragrafens 2 mom. avses med fientlig verksamhet 1) orättmätig militär verksamhet som en främmande stat eller en militär styrka utan beteckningar riktar mot finskt territorium eller som sker på finskt territorium, 2) överskridande av gränsen till finskt territorium av örlogsfartyg eller militära luftfartyg som tillhör en främmande stat eller en militär styrka utan beteckningar eller av ett militärfordon som tillhör en främmande stat eller en militär styrka utan beteckningar trots varning som utfärdats av en territorialövervakningsmyndighet, 3) en främmande stats ubåts eller annat undervattensfordons olovliga ankomst till Finlands territorialvatten annat än i övervattensläge, 4) spaning och elektronisk störning som av en främmande stat eller av en militär styrka utan beteckningar orättmätigt riktas mot på finskt territorium belägna objekt som är viktiga med tanke på rikets säkerhet, 5) elektronisk störning som av en främmande stat eller av en militär styrka utan beteckningar orättmätigt riktas mot ett finländskt statsluftfartyg eller statsfartyg som utför ett territorialövervakningsuppdrag och 6) att en främmande stat eller en militär styrka utan beteckningar orättmätigt utnyttjar finskt territorium vid sådan verksamhet som avses i 1–5 punkten och som riktar sig mot en tredje stat.

Enligt 5 kap. 8 § 4 mom. i polislagen har Polisen rätt att kortvarigt hindra användning av teleadresser eller teleterminalutrustningar inom ett visst område. Åtgärden ska vara nödvändig för att avvärja allvarlig fara som hotar liv eller hälsa och den får inte orsaka större skada eller olägenhet än vad som är nödvändigt för utförande av uppdraget.

I 37 § i lagen om militär underrättelseverksamhet finns det bestämmelser om teleövervakning som används i militär underrättelseverksamhet. Enligt bestämmelsen är det i teleövervakning i militär underrättelseverksamhet dock inte möjligt att hindra användning av teleadress eller teleterminalutrustning.

Enligt specialmotiveringen till bestämmelsen i polislagen (RP 224/2010 rd, s. 102/II) är det inte fråga om att tillfälligt förhindra användningen av en viss teleadress eller teleterminalutrustning som är föremål för teleövervakning utan om att förhindra kortvarig användning av ett okänt antal teleadresser och teleterminalutrustningar, i syfte att avvärja en fara.

I förarbetena till polislagen (RP 224/2010 rd, s. 102/II–103/I) nämns som exempel på användning av befogenheten situationer där man hotat att spränga en bomb på en viss plats eller att en person som deltar i ett internationellt toppmöte veterligen är utsatt för ett allvarligt hot. I sådana situationer kan polisen tillfälligt hindra användning av en teleadress eller en teleterminalutrustning för att hindra att sprängmedlet kan utlösas. För åtgärden uppställs emellertid motsvarande farovillkor som för teleavlyssning. Åtgärden ska vara nödvändig och faran ska vara allvarlig. Intressen som ska skyddas är endast liv och hälsa. Åtgärden får inte heller orsaka större skada eller fara än vad som är nödvändigt för att utföra uppgiften. Genom detta betonas betydelsen av principen om minsta olägenhet vid användning av befogenheten.

Enligt specialmotiveringen har man sålunda uppställt relativt strikta förutsättningar för användning av befogenheten, varför den kan användas endast i exceptionella fall. Dessutom fattas beslut om åtgärden av chefen för centralkriminalpolisen, skyddspolisen eller rörliga polisen eller av chefen för en polisinsättning eller i brådskande fall av en anhållningsberättigad polisman.

I paragrafens 1 och 2 mom. finns det bestämmelser om tillfälligt förhindrande av att enskilda teleadresser eller teleterminalutrustningar används.

I 62 § i lagen om militär underrättelseverksamhet finns det bestämmelser om underrättelseinhämtning som avser utländska datasystem. Enligt dess 1 mom. avses med underrättelseinhämtning som avser utländska datasystem att information inhämtas med

datatekniska metoder från ett datasystem utanför Finland. Enligt paragrafens 2 mom. får Försvarsmaktens underrättelsetjänst rikta underrättelseinhämtning som avser utländska datasystem på ett datasystem, om detta kan antas vara av synnerlig vikt för att inhämta information med avseende på underrättelseuppdraget.

Bestämmelsen omfattar inte på samma sätt som i fråga om teleövervakning någon befogenhet att ingripa i funktionen för ett informationssystem som utgör objekt, även om det orsakar allvarlig fara för Finlands landsförsvar eller den nationella säkerheten.

2.2.8 Underrättelseskyldigheten

I 89 § i lagen om militär underrättelseverksamhet finns det bestämmelser om underrättelse om användning av en metod för underrättelseinhämtning. Enligt paragrafens 1 mom. ska 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 utan dröjsmål underrättas om detta skriftligen efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts.

Enligt regeringens proposition (RP 203/2017 rd, s. 329) uppräknas i momentet de metoder för underrättelseinhämtning 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 förtroliga meddelanden beträffande den person som är föremål för användningen av en metod för underrättelseinhämtning. I paragrafen ska skyldigheten att underrätta föremålet för underrättelseinhämtning om användningen av en metod för underrättelseinhämtning som avses i momentet i princip kopplas till den tidpunkt då denna underrättelseinhämtning har avslutats. En underrättelse som avges först efter denna tidpunkt äventyrar inte pågående underrättelseinhämtning. Underrättelseinhämtningen har kunnat avslutas antingen för att syftet med den har uppnåtts eller för att den har visat sig vara resultatlös.

Underrättelsen ska vara specificerad på ett sådant sätt att föremålet vid behov kan försöka reda ut orsaken till att en metod för underrättelseinhämtning har använts mot honom eller henne. I underrättelsen ska nämnas till exempel vilken metod för underrättelseinhämtning som använts samt var och när den använts. Taktiska och tekniska detaljer om underrättelseinhämtningen behöver myndigheten dock inte avslöja. Underrättelsen till föremålet ska kunna göras till exempel per brev till dennes senast kända adress.

När användningen av en metod för underrättelseinhämtning faktiskt har avslutats innan tillståndets eller beslutets giltighetstid löper ut, och det inte har ansökts om ett nytt tillstånd eller beslutet inte har förlängts, ska underrättelsen till föremålet ges vid den faktiska avslutningstidpunkten. Om informationsinhämtningen fortgår med stöd av ett 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.

Till vem underrättelsen ska göras, avgränsas i praktiken till de egentliga objekten för användningen av en metod för underrättelseinhämtning. Ingen underrättelseskyldighet till en utomstående föreligger till exempel i en situation där man genom teknisk observation av utrustning följer ett sabotageprogram i ett datasystem och det i detta sammanhang blir

nödvändigt att gå igenom e-posten för organisationens arbetstagare för att utreda alla platser till vilka sabotageprogrammet har spridit sig. Ingen underrättelseskyldighet föreligger avseende personer vars e-postkorrespondens det varit nödvändigt att gå igenom, eftersom de inte är objekt för användning av metoden för underrättelseinhämtning.

Å andra sidan får underrättelsemyndigheten inte heller behandla e-postmeddelanden till andra delar än i fråga om sabotageprogrammet. Underrättelsemyndigheten har inte heller tillstånd att inhämta uppgifter till andra delar än avseende sabotageprogrammet. Uppgifter utanför uppgiften om sabotageprogrammet ska utplånas utan oskäligt dröjsmål i enlighet med utplåningsregleringen.

Enligt paragrafens 2 mom. ska underrättelseinhämtning som avser datatrafiken hos andra än statliga aktörer meddelas skriftligen till den person som varit föremål för underrättelseinhämtningen efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts och om identifieringsuppgifterna för eller innehållet i ett konfidentiellt meddelande från en person som vid tidpunkten för genomförandet av underrättelseinhämtningen befann sig i Finland har retts ut manuell vid behandlingen. 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 föreligga någon underrättelseskyldighet redan av den orsaken att detta ofta är omöjligt till exempel för att man inte känner till föremålets riktiga identitet eller för att man inte känner till var föremålet, vars identitet i sig har identifierats, befinner sig eller med ett skäligt arbete kan reda ut det. Ingen underrättelseskyldighet föreligger dock om en uppgift som fåtts genom underrättelseinhämtning som avser datatrafik har utplånats utifrån 86 §.

Enligt regeringens proposition (RP 203/2017 rd, s. 330) 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 innehåller lagen om övervakning av underrättelseverksamheten (121/2019) bestämmelser om en allmän rätt att framföra klagomål eller en begäran om undersökning till underrättelsetillsynsombudsmannen. I Europadomstolens avgörandepraxis har en snävare underrättelseskyldighet ansetts vara godtagbar, om den aktör som upplever att den på omotiverade grunder varit föremål för en underrättelseåtgärd har en omfattande möjlighet att framföra klagomål eller i övrigt överföra sin sak för att prövas av en myndighet som är utomstående i förhållande till underrättelsemyndigheten.

I 7 § i lagen om övervakning underrättelseverksamhet finns det bestämmelser om underrättelsetillsynsombudsmannens uppgifter. Enligt paragrafen har paragrafen har underrättelsetillsynsombudsmannen till uppgift att 1) övervaka lagenligheten vid användning av underrättelseinhämtningsmetoder och underrättelseinformation samt i övrig underrättelseverksamhet, 2) övervaka tillgodoseendet av de grundläggande och mänskliga rättigheterna i underrättelseverksamheten, 3) främja rättssäkerheten och god praxis i anknytning till den i underrättelseverksamheten och 4) inom sitt ansvarsområde ge akt på och bedöma hur verkkningsfull lagstiftningen är och lägga fram de utvecklingsförslag som han eller hon anser vara behövliga. ”I underrättelseverksamhet”, som nämns i bestämmelsen, hänvisar till att underrättelsetillsynsombudsmannen kan övervaka underrättelseverksamheten överlag och inte endast de metoder för underrättelseinhämtning som nämns i lagstiftningen om civil och militär underrättelseinhämtning.

Omfattande och starka befogenheter har föreskrivits i lagen för ombudsmannen för genomförandet av dess uppgifter. Ombudsmannen har bland annat omfattande rättigheter att få

uppgifter och göra granskningar samt rätt att förordna att användningen av en metod för underrättelseinhämtning ska avbrytas och avslutas samt att uppgifter som inhämtats på lagstridigt sätt ska utplånas. Ombudsmannen kan även ge rekommendationer, anvisningar, råd och utlåtanden samt ta initiativ. Ombudsmannen kan till exempel bistå i utarbetandet av granskningsplaner för den interna laglighetsövervakningen och ge råd till underrättelsemyndigheterna i lagenlighetsfrågor. Besvarande av klagomål och begäranden om undersökning är en central del av underrättelsetillsynsombudsmannens verksamhet.

Enligt 89 § 2 mom. i lagen föreligger skyldighet att underrätta underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer emellertid inte, om den information som inhämtats genom underrättelseinhämtning som avser datatrafik har utplånats med stöd av 86 §. Om man vid behandlingen av kommunikationen utrett innehållet i ett meddelande av en viss person som vistas i Finland, men på samma gång upptäckt att uppgiften omfattas av utplåningsskyldigheten, föreligger således ingen underrättelseskyldighet.

I förarbetena till lagen om militär underrättelseverksamhet (RP 203/2017 rd, s. 330) föreslogs att underrättelseinhämtning som avser datatrafik ska underrättas endast till en person som befinner sig i Finland vid tidpunkten för användningen av underrättelseinhämtning som avser datatrafik och som har ett förtroligt meddelande eller lagrad information vars *innehåll* har utretts manuellt. I sitt utlåtande om regeringens proposition ansåg grundlagsutskottet (GrUU 36/2018 rd, s. 27–28) att denna lösning inte var tillräcklig genom att konstatera att identifieringsuppgifter som anknyter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem likväl kan vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde, till vilken det hänvisats i regeringens proposition, inte är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är. Utskottet konstaterade att det exempelvis utifrån geografisk information eller identifieringsuppgifter om besökta webbplatser går att tämligen ingående utreda information som hör till privatlivets kärnområde, till exempel uppgifter om personens politiska övertygelse eller sociala relationer. På grund av detta ansåg utskottet att det var nödvändigt att skyldigheten att underrätta om åtgärder utsträcks också till manuell hantering av identifieringsuppgifter för meddelanden och fastställde att den här ändringen är ett villkor för att lagförslaget ska kunna behandlas i vanlig lagstiftningsordning. På grund av den ändring som grundlagsutskottet förutsatte, utvidgades underrättelseskyldigheten avseende underrättelseinhämtning som avser datatrafik delvis till en okontrollerbar form. Detta har även onödigt ökat uppskoven av underrättelser och de framförda kraven avseende avstående från underrättelse till domstolen.

Enligt paragrafens 3 mom. ska den som varit föremål för inhämtande av information dock underrättas om användningen av metoden för underrättelseinhämtning senast ett år efter det att användningen av metoden upphörde.

I paragrafens 4 mom. föreskrivs att 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.

Enligt 5 mom. ska den domstol som beviljat tillståndet samtidigt skriftligen informeras om underrättelsen.

Enligt paragrafens 6 mom. får domstolen på yrkande av huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman besluta att en underrättelse 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.

Enligt regeringens proposition (RP 203/2017 rd, s. 331–332) ska domstolen 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. 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 till exempel 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. Inhämtandet av information ska kunna anknyta till vilken som helst pågående underrättelseoperation, också till en civil underrättelseoperation.

Uppskov ska också vara möjligt med tanke på landets försvar eller skyddandet av den nationella säkerheten. Detta innebär att det måste föreligga 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.

Underrättelsen får utifrån en domstols beslut 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.

Det kan anses att momentets betydelse är accentuerad vid militär underrättelseinhämtning. På ovan konstaterade sätt har den principiella underrättelseskyldigheten, som i synnerhet i fråga om underrättelseinhämtning som avser datatrafik utvidgats till en okontrollerbar form, lett till att bestämmelsen tillämpas i relativt omfattande grad.

Enligt paragrafens 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, om förundersökning inte har inletts i ärendet utifrån en i 79 eller 80 § avsedd anmälan. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen (806/2011) iakttas.

Enligt regeringens proposition (RP 203/2017 rd, s. 332) ska en underrättelse i fråga om platsspecifik underrättelseinhämtning göras till den som varit föremål för den ifrågavarande metoden för underrättelseinhämtning och vid behov även till ägaren eller innehavaren av platsen. 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 militärunderrättelsemyndigheterna, ska informationen kunna ges i enlighet med det förfarande om vilket föreskrivs i 76 och 77 §. Om förundersökning inleds utifrån information som getts enligt vad som föreskrivs i 76 eller 77 §, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen iakttas.

Enligt momentet behöver underrättelse inte göras om användning av de i momentet nämnda metoderna för underrättelseinhämtning, om förundersökning inte ska inledas i det ärende som gäller metoderna i fråga.

Enligt paragrafens 8 mom. behöver den som varit föremål för användningen av en metod för underrättelseinhämtning inte underrättas om detta, om föremålet har varit en statlig aktör.

Enligt paragrafens 9 mom. ska i fråga om handläggning av underrättelseärenden i domstol 116 § iakttas.

2.2.9 Deltagande av utomstående i förhållande till en militärunderrättelsemyndighet i militär underrättelseverksamhet

Övriga myndigheters deltagande

I 18 § i lagen om militär underrättelseverksamhet finns det bestämmelser om samarbete med andra myndigheter och med företag och andra sammanslutningar. Enligt paragrafens 1 mom. ska militärunderrättelsemyndigheterna 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, trots sekretessbestämmelserna lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten. Bestämmelser om utlämnande av personuppgifter finns i lagen om behandling av personuppgifter inom Försvarsmakten.

Enligt paragrafens 2 mom. kan militärunderrättelsemyndigheterna för att genomföra sitt uppdrag trots sekretessbestämmelserna till företag och andra sammanslutningar lämna ut identifieringsuppgifter som anknyter till sabotageprogram och som behövs för utvecklingen av metoder och system för underrättelseinhämtning eller lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är nödvändigt med avseende på Försvarsmaktens verksamhet eller för att skydda den nationella säkerheten.

Enligt paragrafens 3 mom. innehåller lagens 6 kap. bestämmelser om utlämnande av information för brottsbekämpning och enligt paragrafens 4 mom. får närmare bestämmelser om organiserandet av samarbetet mellan militärunderrättelsemyndigheterna och andra myndigheter samt om vilka som ska delta i samarbetet och om deras uppgifter genom förordning av statsrådet.

Deltagande av aktörer som står utanför myndigheterna i underrättelseverksamhet

I 51 § i lagen om militär underrättelseverksamhet finns det bestämmelser om användning av informationskällor. Enligt paragrafens 1 mom. avses med användning av informationskällor annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av underrättelseuppdrag av personer som inte hör till en finsk myndighet (*informationskälla*).

Enligt paragrafens 2 mom. får militärunderrättelsemyndigheterna 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.

Enligt paragrafens 3 mom. får man vid styrd användning av informationskällor inte begära att uppgifter inhämtas på ett sådant sätt som förutsätter utövning av myndighetsbefogenheter eller som äventyrar informationskällans eller någon annans liv eller hälsa. Innan styrd användning av en informationskälla inleds, ska informationskällan få en redogörelse över hans eller hennes rättigheter och skyldigheter och i synnerhet om verksamhet som enligt lag är tillåten och förbjuden för honom eller henne. Informationskällans säkerhet ska vid behov tryggas under och efter inhämtandet av information. Det står klart att det inte är möjligt att tilldela en informationskälla uppgifter med vilka användningen av de befogenheter som getts till myndigheter kringgås. Till exempel inhämtning av information från ett utrymme som används för boende av permanent natur kan inte göras genom att använda en informationskälla. På motsvarande sätt, med undantag för ombesörjande av en informationskällas säkerhet, kan en informationskälla inte försees med en anordning som möjliggör teknisk observation och avlyssning.

En informationskälla kan inte användas för annat än att förmedla uppgifter som han eller hon fått i sin normala verksamhet genom att använda sina normala sociala förhållanden. Till exempel i en situation där en informationskälla beviljats tillträde till ett visst utrymme och till vissa anordningar, kan informationskällan inte installera en programvara, metod eller anordning som behövs för att använda metoder för militär underrättelseinhämtning.

Vid användning av informationskällor ska man beakta risken för deltagande i kriminell verksamhet, vilken i praktiken kan bli verklighet i och med att informationskällan styrs att inhämta information från ett plats dit han eller hon har tillträde endast genom att använda kriminella metoder. Detta har gått igenom närmare i samband med tvångsmedlen. Till exempel 10 kap. 28 § 1 mom. i tvångsmedelslagen, vilket gäller täckoperationer, innehåller ett uttryckligt förbud att begå brott eller ta initiativ för att begå brott. I paragrafens 2 mom. föreskrivs att trots vad som föreskrivs i 1 mom. får en polisman som företar en täckoperation begå en ordningsförseelse eller något annat jämförbart brott, för vilket det föreskrivna straffet är ordningsbot, eller en trafikförseelse, om gärningen är nödvändig för att syftet med täckoperationen ska nås eller för att inhämtandet av information inte ska avslöjas.

Enligt förarbetena till tvångsmedelslagen hänvisade 28 § 2 mom. och 29 § 1 mom. till en bedömning och prövning som görs i förväg och planmässigt. Dessutom förutsätter 29 § 1 mom. 1 punkten att synnerligen giltiga grunder föreligger vid den tidpunkt då åtgärden vidtas, med stöd av vilka det kan förmodas att den kriminella åtgärden hade vidtagits utan medverkan av en polis som arbetar under täckmantel. Åtgärdens godtagbarhet bedöms i princip och i mån av möjlighet innan verksamheten inleds, då beslutet om användningen av tvångsmedlet bereds (RP 217/2022 rd, s. 55, se även RP 222/2010 rd, s. 351–352). Såväl i 28 § 2 mom. som i 29 § 1 mom. handlar det om bestämmelser som skrivits i form av befogenhetsreglering, som reglerar

vad en polisman som utför täckoperationer får göra i de situationer och under de förutsättningar vilka närmare fastställs i bestämmelserna (RP 217/2022 rd, s. 55).

Även i fråga om militär underrättelseverksamhet kan man i fråga om användning av informationskällor anse att utgångspunkten är att om informationskällan agerar i strid med hans eller hennes anvisningar eller enligt egen prövning eller utifrån ett eget beslut deltar i annan än den verksamhet som anvisningarna gäller, är det möjligt att han eller hon eventuellt har straffrättsligt ansvar för sina åtgärder. I dessa situationer torde ärendet i den senare straffprocessen dock bli föremål för en separat bedömning som gäller exempelvis regleringen om grunderna för ansvarsfrihet enligt 4 kap. i strafflagen (förbudsvillfarelse, berättigande grund, ursäktlighetsgrund). Det bör observeras att en lagstridig gärning kan bli känd först efter en lång tid.

Också brottsprovokation är en särskild fråga.

Användning av informationskällor enligt lagen ska åtskiljas från bistånd till en myndighet. En privatperson kan frivilligt vilja ställa till exempel sin sommarstuga till militärunderrättelsemyndighetens förfogande för en kort tid till exempel som stödpunkt för en underrättelseoperation i ett lagerutrymme. Det står klart att en militärunderrättelsemyndighets inhämtande av information inte heller i dessa situationer kan hänföra sig till ett hemfridsskyddat utrymme och det handlar inte heller om bistånd.

Enligt den gällande inkomstskattelagen kan ett arvode betalas skattefritt till en informationskälla. Bakgrunden till regleringen utgörs av skyddet av liv och hälsa.

I 2 kap. 17 § 3 mom. i polislagen har den som på begäran eller med samtycke av en polisman tillfälligt bistår en polisman i en situation där det är nödvändigt att anlita utomstående hjälp vid användning av maktmedel för att utföra ett synnerligen viktigt och brådskande polisiärt tjänsteuppdrag, rätt att under polismannens uppsikt använda maktmedel som polismannen med stöd av sina befogenheter bemyndigar honom eller henne att använda.

Enligt 9 kap. 3 § 1 mom. i polislagen är var och en skyldig att på befallning av en polisman som hör till befälet bistå polisen med att leta efter personer som har försvunnit och befinner sig i livsfara, med att rädda människoliv, hjälpa skadade samt avvärja betydande skada på egendom eller miljön, om deltagandet i en sådan åtgärd inte är oskäligt med hänsyn till vederbörandes ålder, hälsotillstånd eller personliga förhållanden eller av andra särskilda skäl.

I paragrafens 2 mom. föreskrivs att i sådana fall som avses i 1 mom. samt vid letande efter drunknade ska privatpersoner och privata sammanslutningar på befallning av en polisman som hör till befälet i skälig utsträckning och mot full ersättning ställa livsmedel, telekommunikationsmedel, transportmedel, arbetsredskap samt andra behövliga apparater och ämnen till polisens förfogande.

I 8 kap. i lagen om militär underrättelseverksamhet finns det bestämmelser om Försvarsmaktens tjänstemäns och värnpliktigas deltagande i militär underrättelseinhämtning. Kapitlet innehåller bestämmelser om Försvarsmaktens tjänstemäns deltagande i militär underrättelseinhämtning, befogenheter för en reservist som tjänstgör i enlighet med värnpliktslagen, deltagande i Försvarsmaktens internationella verksamhet och tjänsteansvar för den som tjänstgör i enlighet med värnpliktslagen.

Enligt 91 § 1 mom. i lagen om militär underrättelseverksamhet får en reservist som deltar i en repetitionsövning i enlighet med värnpliktslagen (1438/2007) och som har fått tillräcklig

utbildning bistå militärunderrättelsemyndigheterna vid radiosignalspaning, underrättelseinhämtning som avser utländska datasystem, behandling av tekniska data och inriktning av underrättelseinhämtning som avser datatrafik.

Enligt paragrafens 2 mom. får 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, 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.

Enligt paragrafens 3 mom. får en reservist som i enlighet med 47 § i lagen om försvarsmakten (551/2007) har tagit avsked från en militärunderrättelsemyndighet och som deltar i en repetitionsövning enligt värnpliktslagen använda de metoder för underrättelseinhämtning som avses i 4 kap.

Enligt paragrafens 4 mom. får en reservist 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.

I 95 § i lagen om militär underrättelseverksamhet finns det bestämmelser om yppandeförbud. I dess 1 mom. föreskrivs att för en 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.

Enligt motiveringarna till den andra meningen i momentet är förutsättningen att en utomstående på grund av sitt uppdrag eller sin ställning gett bistånd eller ombetts att ge bistånd i användningen av en metod för underrättelseinhämtning. Ett yppandeförbud kan således ges vem som helst, till exempel invånarna i ett husbolag eller andra utomstående som av slumpen ser installationen av en anordning för teknisk observation. I bestämmelsen avses med användning av en metod för underrättelseinhämtning användning av metoder för underrättelseinhämtning i en bredare mening, som omfattar exempelvis skydd av användning av metoder för underrättelsemetod som används i militär och civil underrättelseinhämtning då militärunderrättelsemyndigheten och skyddspolisens samarbetar. Det är befogat att meddela ett yppandeförbud åtminstone då användningen av en metod för underrättelseinhämtning kan röjas utan att förbudet meddelas till utomstående.

Utländsk tjänsteman

I 20 § i lagen om militär underrättelseverksamhet finns det bestämmelser om internationellt samarbete. Enligt paragrafens 1 mom. kan militärunderrättelsemyndigheterna i enlighet med Finlands nationella intressen i anknytning till sina uppgifter eller för att skydda den nationella säkerheten 1) trots sekretessbestämmelserna utbyta andra underrättelseuppgifter än personuppgifter med utländska underrättelse- och säkerhetstjänster eller med Nordatlantiska fördragsorganisationen eller någon annan internationell organisation eller med Europeiska

unionen, om det behövs, och 2) delta i internationellt samarbete i anknytning till inhämtandet och bedömningen av underrättelseuppgifter.

I paragrafens 2 mom. föreskrivs att 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.

I paragrafens 3 mom. föreskrivs att en behörig utländsk tjänsteman genom beslut av huvudstabens underrättelsechef har 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 22, 24, 43, 47, 51, 60 och 66 §. En utländsk tjänsteman är skyldig att iaktta föreskrifter, begränsningar och anvisningar som en militärunderrättelsemyndighet gett honom eller henne.

I paragrafens 4 mom. föreskrivs att huvudstabens underrättelsechef beslutar om deltagande i internationellt samarbete och om användning av metoderna för underrättelseinhämtning.

I paragrafens 5 mom. föreskrivs att internationellt samarbete är förbjudet om det finns grundad anledning att misstänka att en person på grund av samarbetet eller utlämnandet av uppgifter riskerar dödsstraff, tortyr, någon annan behandling som kränker människovärdet, förföljelse, godtyckligt frihetsberövande eller orättvis rättegång.

I paragrafens 6 mom. föreskrivs att vid utlämnande och mottagande av uppgifter enligt denna paragraf iaktas 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). Bestämmelser om utlämnande av personuppgifter finns i lagen om behandling av personuppgifter inom försvarsmakten.

I paragrafens 7 mom. föreskrivs att huvudstabens underrättelsechef beslutar om användning inom finskt territorium av radiosignalspaning enligt 60 § som genomförs av Nordatlantiska fördragsorganisationen eller dess medlemsstater från fordon, fartyg eller luftfartyg eller från markstationer. Det samarbete som avses i detta moment ska vara förenligt med Finlands intressen och de prioriteringar som avses i 13 § samt ske under ledning och övervakning av en militärunderrättelsemyndighet.

I enlighet med paragrafen utgörs utgångspunkten för internationellt samarbete av Finlands nationella intresse och vid verksamhet med stöd av paragrafen ska Finland få en fördel som gäller landets försvar och den nationella säkerheten.

När en utländsk tjänsteman agerar i biträdande uppgifter enligt 3 mom. i paragrafen, fattas beslutet om och beviljas tillståndet till den egentliga metoden för underrättelseinhämtning enligt vad som föreskrivits om användningen av den aktuella metoden för underrättelseinhämtning.

2.2.10 Tryggande av informationskällor

Användning av informationskällor kan ses som en central metod för underrättelseinhämtning. De bästa informationskällorna kan producera den allra djupaste informationen och information om de allra hemligaste ärendena. Informationskällorna utsätter även sitt eget liv och sin egen hälsa för fara då de fungerar som informationskällor. På grund av detta ska underrättelsemyndigheten i tillräcklig mån sörja för informationskällans säkerhet.

I 78 § i lagen om militär underrättelseverksamhet finns det bestämmelser om tryggnad av informationskällor. Enligt paragrafens 4 mom. får en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman 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. En registeranteckning ska rättas efter att förutsättningarna enligt detta moment inte längre föreligger.

Det kan vara utmanande att trygga en informationskälla utomlands i en situation där informationskällan har lämnat uppgifter till en finländsk militärunderrättelsemyndighet från utlandet, varvid det ändamålsenligaste sättet att trygga informationskällan kan vara att få ut informationskällan ur landet. I vissa situationer kan det även finnas ett behov av att göra arrangemang för att informationskällan ska kunna korsa den finländska gränsen via andra än officiella gränsövergångsställen eller på dolt sätt via ett officiellt gränsövergångsställe. Om en informationskällas liv och hälsa är i fara, kan han eller hon naturligtvis inte komma till Finland längs officiella ruttor, varför den finländska militärunderrättelsemyndigheten ska ge hjälp till exempel genom att i enlighet med 78 § 4 mom. i lagen om militär underrättelseverksamhet ge uppgifter eller falska handlingar till informationskällan då han eller hon passerar gränsen.

Det finns bestämmelser om riksgränsbrott i 17 kap. 7 § i strafflagen. I dess 1 mom. föreskrivs att den som 1) överskrider eller försöker överskrida Finlands gräns utan att inneha ett till detta berättigande resedokument, visum, uppehållstillstånd eller något annat dokument som kan jämföras med ett resedokument, eller som överskrider eller försöker överskrida gränsen någon annanstans än genom ett tillåtet inrese- eller utreseställe eller i strid med ett annat på lag grundat förbud än ett inreseförbud, 2) annars bryter mot bestämmelserna om överskridande av gränsen, eller 3) i strid med 51 § i gränsbevakningslagen eller utan tillstånd som avses i 52 § i den lagen vistas eller färdas inom gränzonen eller vidtar någon åtgärd som är förbjuden inom den, ska för *riksgränsbrott* dömas till böter eller fängelse i högst ett år.

Enligt paragrafens 2 mom. döms för riksgränsbrott inte en utlänning som med anledning av en sådan gärning som avses i 1 mom. avvisas eller utvisas och inte heller en utlänning som på grund av flyktingskap ansöker om asyl eller uppehållstillstånd i Finland. För riksgränsbrott döms inte heller en utlänning som har begått ett brott enligt 1 mom. till följd av att han eller hon har varit föremål för människohandel enligt 25 kap. 3 eller 3 a §.

Det finns bestämmelser om ordnande av olaglig inresa i 17 kap. 8 § i strafflagen. Enligt bland annat 1 mom. 2 punkten ska den som för in eller försöker föra in en sådan utlänning i Finland, eller genom Finland till ett annat land, som har ett i 1 punkten avsett dokument som är falskt eller förfalskat eller har beviljats någon annan, eller som har fått av en myndighet genom att ge osanna eller vilseledande uppgifter som är betydelsefulla för beviljandet av dokumentet, genom att muta myndigheten eller genom våldsam motstånd mot tjänsteman för ordnande av olaglig inresa dömas till böter eller fängelse i högst två år.

2.2.11 Platsspecifik underrättelseinhämtning och kopiering

Det finns bestämmelser om platsspecifik underrättelseinhämtning i 54 § i lagen om militär underrättelseverksamhet. Enligt paragrafen avses med platsspecifik underrättelseinhämtning underrättelseinhämtning för att hitta föremål, egendom, handlingar eller information eller utröna omständigheter i något annat utrymme än ett utrymme som används för boende av permanent natur 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.

Det finns bestämmelser om beslut om platsspecifik underrättelseinhämtning i 55 § i lagen om militär underrättelseverksamhet. Enligt paragrafens 1 mom. ska beslut om platsspecifik underrättelseinhämtning fattas av domstol när den riktas 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.

Enligt specialmotiveringen till bestämmelsen (RP 203/2017 rd, s. 274) föreskrivs i 3 mom. i paragrafen att huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman beslutar om platsspecifik underrättelseinhämtning enligt 1 mom. 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. Dessutom omfattar momentet sådana fordon som inte används för boende av permanent natur.

I 56 § i lagen om militär underrättelseverksamhet finns det bestämmelser om kopiering. Enligt paragrafen har militärunderrättelsemyndigheterna rätt att kopiera ett dokument eller ett annat föremål för utförande av ett underrättelseuppdrag. Kopieringen kan göras och görs även ofta i samband med platsspecifik underrättelseinhämtning. Kopiering kan även bli aktuellt till exempel i samband med att befogenheten till systematisk observation utövas.

I specialmotiveringen till kopieringsbestämmelsen (RP 203/2017 rd, s. 275) nämns som exempel på kopiering av ett dokument att man fotograferar eller skannar dokumentet med hjälp av ett skanningsprogram som installerats i en telefon eller att ett föremål kopieras med användande av en 3D-skanner.

Kopieringsbestämmelsen möjliggör inte att prover tas från ämnen, egendom eller föremål som hittats i samband med platsspecifik underrättelseinhämtning eller en annan metod för underrättelseinhämtning och inte heller att sådana omhändertas för provtagning eller för att göra dem ofarliga.

Enligt specialmotiveringen till bestämmelsen om platsspecifik underrättelseinhämtning (RP 203/2017 rd, s. 274) är det inte heller vid platsspecifik underrättelseinhämtning tillåtet att omhänderta föremål, dokument eller annan egendom som finns i utrymmet, utan nödvändig information om dem ska lagras till exempel 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.

2.2.12 En militärunderrättelsemyndighets rätt att få uppgifter

I 17 § i lagen om försvarsmakten finns det bestämmelser om rätten att få information för Försvarsmakten, inbegripet en militärunderrättelsemyndighet. Enligt paragrafen har Försvarsmakten rätt att trots sekretessplikten av myndigheter och av sammanslutningar som tillsatts för att sköta ett offentligt uppdrag få de uppgifter och handlingar som är nödvändiga för skötseln av lagstadgade uppdrag, om inte lämnandet av uppgiften eller handlingen till Försvarsmakten eller användningen av uppgifterna som bevis har förbjudits eller begränsats i lag.

Den allmänna rätten att få information för en militärunderrättelsemyndighet kompletteras av 37 § i lagen om behandling av personuppgifter inom Försvarsmakten. Enligt 1 mom. 17 punkten i den har Försvarsmakten utöver vad som föreskrivs någon annanstans i lag, för fullgörande av uppdrag inom militär underrättelseinhämtning samt uppdrag för förhindrande och avslöjande av brott som avses i 86 1 mom. i lagen om militär disciplin och brottsbekämpning inom Försvarsmakten trots sekretessbestämmelserna rätt att trots sekretessbestämmelserna få behövliga uppgifter från Skatteförvaltningen ur beskattningens datasystem.

Det finns bestämmelser om fullgöranderapporter i lagen om Enheten för utredning av grå ekonomi (1207/2010). Lagens 5 § innehåller bestämmelser om fullgöranderapporter, medan 6 § reglerar användningsändamålet. Enligt 6 § 1 mom. 39 punkten i lagen utarbetas en fullgöranderapport för att stödja skyddspolisens uppgifter när det gäller att skydda den nationella säkerheten mot verksamhet som utgör ett allvarligt hot mot den.

Enligt 7 § 1 mom. i lagen om Enheten för utredning av grå ekonomi har utredningsenheten rätt att trots sekretessplikten av myndigheterna få de uppgifter som är nödvändiga för utarbetandet av en fullgöranderapport och som den myndighet som begär rapporten har rätt att få för det ändamål som uppges i begäran. Bestämmelsen ändrar således inte rätten till sekretessbelagda uppgifter för den myndighet som begärt en utredning till.

Polisens allmänna rätt till information föreskrivs i 2 § 1 mom. i polislagen. Polisens allmänna rätt till information kan dock begränsas av en bestämmelse som ska tillämpas som en specialbestämmelse i förhållande till polislagen, där rätten att lämna ut uppgifter har avgränsats på ett noggrant avgränsat endast till vissa användningsändamål. Som sammandrag av vad som ovan konstaterats om regleringen möjliggör de centrala bestämmelserna om socialförsäkring i fråga om en fullgöranderapport att uppgifter lämnas ut till förundersökningsmyndigheterna för att förebygga och utreda brott. Således hade skyddspolisen utan den uttryckliga författningsändringen inte kunnat få behövliga uppgifter för att trygga den nationella säkerheten, eftersom skyddspolisen ses som polisen.

2.2.13 Underrättelseinhämtning från öppna källor

Underrättelseinhämtning från öppna källor (Open source intelligence, OSINT) är ett slag av underrättelseinhämtning som är tillåtet utifrån sedvanerätten (se LaUB 44/2010 rd, s. 26). Information i öppna källor är avsedda för allmänheten och även tillgänglig för var och en. Inhämtande av information från öppna källor av en enskild tjänsteman innebär i princip inte något ingrepp i de grundläggande fri- och rättigheterna och de mänskliga rättigheterna och därför har det hittills inte ansetts föreligga något behov av att utfärda bestämmelser om detta genom lag.

Inhämtande av information från öppna källor kan användas till stöd för andra metoder för underrättelseinhämtning eller som en självständig metod för att inhämta information till exempel i situationer där det inte är möjligt eller effektivt att använda andra metoder för underrättelseinhämtning (se till exempel RP 203/2017 rd, s. 225). Inhämtande av information kan grovt sett delas in i underrättelseinhämtning som baserar sig på en avgränsad underrättelsefråga och till exempel bevakning av medier.

Till fördelarna med inhämtande av information från öppna källor hör att den är snabb, billig och geografiskt obegränsad samt att information kan samlas in även om kommande händelser (se RP 203/2017 rd, s. 226). Betydelsen av öppna källor för underrättelseinhämtningen och myndighetsverksamheten är avsevärd, och genom information som fås från öppna källor är det även möjligt att komplettera annan underrättelseinformation och vice versa. Det har även

allmänt ansetts att det är möjligt att i större utsträckning dela analyserad information som baserar sig endast på öppna källor.

Genom att leta efter och kombinera inhämtad information är det möjligt att bilda helheter som berättar mer om verksamheten än vad som annars vore möjligt. Inhämtande av information från öppna källor förutsätter att informationen delas in på ett enhetligt sätt, bedöms omsorgsfullt och filtreras. Avigsidan med den stora mängden informationen är att den väsentliga informationen drunknar i massan. Dessutom ska man beakta desinformationsrisken i anknytning till öppna källor. I synnerhet utomlands kan det vara svårt att identifiera relevanta och pålitliga källor ur det stora informationsutbudet.

Typiska informationskällor har varit bland annat litteratur, statistik, kartor, tidningar, publikationer av privatpersoner och myndigheter, myndigheternas offentliga register och databaser, televisions- och radiosändningar riktade till allmänheten samt innehåller i datanät och sociala medier (RP 203/2017 rd, s. 225). Under de senaste åren har i synnerhet antalet observationer via sociala medier ökat i förhållande till andra källor. Till exempel på sociala medier kan en bild som en kontoanvändare tagit av sig själv vara intressant på grund av vad som syns i bildens bakgrund och var och när bilden har tagits. Vad gäller den senaste tidens utveckling bör det konstateras att de ryska krigsbloggarna haft en accentuerad ställning i spridningen av information om kriget i Ukraina.

Information från öppna källor kan inhämtas till exempel genom att köpa spårnings- och analystjänster som gäller källorna eller utredningar om sådana från företag. Dessutom är det möjligt att använda olika programvaror, som gallrar väsentlig information från offentliga källor samt uppdateringar och andra förändringar i dessa. Det centrala målet för underrättelsemyndigheten är att kombinera information från öppna källor med användning av övriga metoder för underrättelseinhämtning och det internationella informationsutbytet för att bilda en mer detaljerad uppfattning eller lägesbild. Information som fås från öppna källor är även en bra metod för att säkerställa att information som fås genom att använda metoder för underrättelseinhämtning eller informationsutbyte är pålitlig.

Inhämtande av information från öppna källor innefattar inte något aktivt deltagande i en diskussion som förs på till exempel en webbplats eller på sociala medier i syfte att inhämta information. Det typiska för inhämtande av information från öppna källor i datanät är att man ska registrera sig till olika tjänster med sådana uppgifter som inte avslöjar syftet med inhämtandet av information eller den som inhämtar den. En ansökan till en sluten grupp av användare på sociala medier, vilken kräver ett godkännande av till exempel gruppadministratören, är på motsvarande sätt en tillåten form av inhämtande av information från öppna källor, om den myndighet som inhämtar informationen vilseleder gruppadministratören att tro att det handlar om någon annan än den verkliga personen. En polisman får dock inte föra en aktiv diskussion med andra medlemmar av en grupp, varvid det kan handla om till exempel förtäckt inhämtande av information eller användning av täckoperationer på nätet. När vilseledningen inte hänför sig till en person, utan till ett datasystem, är situationen en annan. Även en ansökan till olika tjänster i ett datanät, såsom ett diskussionsforum eller en köp- och säljsida på darknet, har ansetts vara tillåtet i egenskap av inhämtande av information från öppna källor. I en sådan situation kan vilseledningen hänföra sig till tjänsteleverantören, såsom administratören av en köp- och säljsida på darknet. Upplägget kan jämföras med att en civilklädd polisman köper en biljett och besöker ett allmänt evenemang, till exempel en musikfestival, och döljer sin ställning som polis.

Inhämtandet av information från öppna källor i ett allmänt datanät kan hänföra sig till information som finns i profilerna för personer som finns i tjänster på sociala medier. Människor

publicerar i datanät och i synnerhet på sociala medier en stor mängd information som gäller dem själva och deras livsmiljö och som omfattas av skyddet av deras integritet. Till exempel kan en person publicera fotografier av sitt hem, sin sommarstuga, sin familj och sina kompisar på ett eget konto på sociala medier. Det har ansetts vara tillåtet att leta efter information från öppna källor, om letandet riktar sig till information som en person publicerat så att den är tillgänglig för allmänheten. Inhämtande av information från öppna källor får dock inte användas för att kringgå en annan befogenhet.

När man agerar i ett datanät ska man i princip alltid sträva efter att radera sitt så kallade digitala fotavtryck, så att en tjänsteman som utnyttjar öppna källor inte kan kopplas samman till den myndighet som inhämtar information.

Vid Försvarmakten kan underrättelseinhämtning från öppna källor användas i stor utsträckning i alla uppgifter som hör till Försvarmakten. Försvarmaktens arbetsordningar och föreskrifter fastställer närmare i vilka samband information kan inhämtas. Det står klart att till exempel personuppgifter inte kan lagras i alla kontexter, utan att ett tydligt skäl ska finnas för det.

I 75 § i lagen om militär underrättelseverksamhet finns det bestämmelser om skyddande av militär underrättelseinhämtning. Enligt paragrafens 1 mom. får militärunderrättelsemyndigheterna använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt upprätta och använda falska handlingar, när det är nödvändigt för att förhindra att den militära underrättelseinhämtningen avslöjas.

Enligt paragrafens 2 mom. ska en registeranteckning som avses i 1 mom. rättas när förutsättningarna enligt det momentet inte längre föreligger.

Enligt paragrafen 3 mom. får närmare bestämmelser om organiserandet av skyddandet av militär underrättelseinhämtning, om den tjänsteman som ansvarar för skyddandet och om samarbetet med personuppgiftsansvariga utfärdas genom förordning av statsrådet.

2.2.14 Rekrytering hos Försvarmakten

Vid försvarsförvaltningen är framför allt den militära underrättelseverksamheten, i egenskap av verksamhet som ska hemlighållas, en metod för att göra observationer och i förväg inhämta information om hot mot den nationella säkerheten. Information inhämtas också om hot som uppstår utanför Finland och som riktar sig mot Finland. Inhämtandet av information hänför sig till objekt som föreskrivs i 4 § i lagen om militär underrättelseverksamhet och som genomförs med de befogenheter som föreskrivs i 4 kap. i lagen (metoder för underrättelseinhämtning). Försvarmaktens uppgifter täcker även i bred skala annan verksamhet, såsom brottsbekämpning, cyberförsvar och uppgifter i anknytning till Försvarmaktens operativa och övriga säkerhet.

Den verksamhet som främmande stater riktar mot Finland är planmässig och långsiktig. De har som mål att försvaga Finlands landsförsvar och i värsta fall göra funktionerna ineffektiva, göra det avsevärt svårare att utföra uppgifter eller överlag göra det omöjligt att utföra uppgifter. I ett stort antal uppgifter är informationen om Försvarmaktens personal och deras arbetsuppgifter i princip sekretessbelagd. Offentlighet för personalinformation bildar i vissa situationer en risk på organisationsnivå för Försvarmakten på grund av eventuella värningsförsök eller andra operationer av en främmande stat mot Försvarmaktens personal.

De som innehar tjänster hos Försvarsmakten har inom ramen för sina uppdrag tillgång till sekretessbelagda uppgifter som ska anses vara kritiska för försvaret av landet och den nationella säkerheten. Oberoende av orsaken till att dessa uppgifter når en extern aktör, kan dessa uppgifter orsaka skada för landets försvar och den nationella säkerheten. Utomstående, fientliga aktörer kan i synnerhet antas vara intresserade av tjänstemän som arbetar i operativa underrättelseuppdrag och anknyttande stöduppgifter eller som arbetar med dataanalys och i tekniska uppgifter. Offentligheten för personens uppgifter möjliggör att ett hot riktas mot en tjänsteman som utför uppgifter relaterade till Försvarsmaktens verksamhet, i värsta fall ett konkret hot mot livet och hälsan. Även ovan nämnda tjänstemäns närkrets och personer som samarbetar med den militära underrättelsen och Försvarsmaktens brottsbekämpning, såsom informationskällor, kan utsättas för risker. Underrättelsetillsynsombudsmannen har mer ingående behandlat hoten mot tjänstemännen hos en underrättelsemyndighet och personer som stadigvarande är i kontakt med dem i sina berättelser för åren 2019⁶ och 2020⁷.

I statstjänstemannalagen (750/1994), som är en allmän lag som gäller för alla statstjänstemän, föreskrivs om förfarandet vid sökande och utnämning till tjänster och till tjänsteförhållanden för viss tid. I princip tillämpas statstjänstemannalagen på Försvarsmaktens ansökningsförfaranden, varvid ett ansökningsförfarande i regel är offentligt.

Enligt 6 a § i statstjänstemannalagen ska en tjänst förklaras ledig att sökas innan den tillsätts. Enligt 6 c § i statstjänstemannalagen ska i ett meddelande om att en tjänst är ledig, det vill säga en utlysning, anges de uppgifter som hör till tjänsten samt de föreskrivna behörighetsvillkoren, dagen då ansökningstiden går ut och den myndighet till vilken ansökan ska riktas. I meddelandet ska vidare nämnas huruvida tjänsten har inrättats vid en särskild enhet eller om den är gemensam för ämbetsverket. Finansministeriet har den 28 oktober 2024 utfärdat en anvisning⁸ om de principer som ska iaktas vid tillsättning av tjänster. I anvisningen anges de övriga omständigheter som ska nämnas i en utlysning.

Utnämningsspromemorian utgör grunden för de motiveringar som läggs fram i utnämningsbeslutet, och promemorian är relevant även när man utreder om lagen om jämställdhet mellan kvinnor och män (609/1986) har följts och med tanke på de rättsmedel som anges i diskrimineringslagen (1325/2014). Motiveringen för det utnämningsbeslut som gäller tillsättning av en tjänst eller ett tjänsteförhållande ska framgå tillräckligt tydligt och transparent av utnämningsspromemorian.

Enligt 6 d § 2 mom. i statstjänstemannalagen ska den myndighet som har fattat utnämningsbeslutet utan dröjsmål lämna dem som har sökt tjänsten eller tjänsteförhållandet ett meddelande om utnämningen. I meddelandet ska nämnas den tjänst eller det tjänsteförhållande som tillsätts, vilken myndighet som har fattat beslutet, datum för utnämningen samt vem som har utnämnts till tjänsten eller tjänsteförhållandet. Enligt 59 § 1 mom. i statstjänstemannalagen får den som söker en tjänst genom besvär söka ändring i ett beslut om utnämning till tjänsten eller tjänsteförhållandet, om inte något annat föreskrivs i den lagen. Besvärstiden börjar från delfåendet av utnämningsbeslutet. Utnämningsbeslutet ska uppfylla de krav som i 44 § i förvaltningslagen (434/2003) ställs på skriftliga förvaltningsbeslut. I beslutet ska nämnas den myndighet som har fattat beslutet samt tidpunkten för beslutet, motiveringen för beslutet och uppgift om den som har utnämnts samt namn på och kontaktuppgifter för den person av vilken

⁶ [Underrättelsetillsynsombudsmannens berättelse från år 2019](#). K 14/2020 rd.

⁷ [Underrättelsetillsynsombudsmannens berättelse från år 2020](#). K 10/2021 rd.

⁸ [Anvisning om de principer som ska iaktas när tjänster tillsätts](#) VN/30496/2024. Finansministeriet.

en part vid behov kan begära ytterligare upplysningar om beslutet. Namnen på de övriga sökandena kan framgå av sändlistan för beslutet. Till ett utnämningsbeslut ska fogas en besvärсанvisning eller en upplysning om besvärsförbud. Parter i utnämningsbeslutet är den person som utnämnts till tjänsten och de övriga sökandena.

Lagstiftningen innehåller dock undantag. Enligt 59 § 2 mom. i statstjänstemannalagen får beslut inte överklagas genom besvär, om det är republikens president eller, vid utnämning av högre tjänstemän vid ministerierna eller av sådana chefer för ämbetsverk som anges i statsrådets förordning, statsrådets allmänna sammanträde som har utnämningsbehörighet. Besvärsrätt föreligger inte heller om en person utnämns för viss tid, högst två år, eller om tjänsten eller tjänsteförhållandet med stöd av lag tillsätts utan att tjänsten eller tjänsteförhållandet ledigförklaras eller om beslutet gäller en militär tjänst inom försvarsmakten eller gränsbevakningsväsendet som med stöd av lag får tillsättas utan att den ledigförklaras. I fråga om militära tjänster gäller besvärsförbudet även om tjänsten tillsätts i ett öppet ansökningsförfarande.

Vid Försvarsmakten finns det personer som tjänstgör i militära tjänster och i civila tjänster. Dessutom kan det finnas personal i ett tjänsteförhållande för viss tid och personal som är anställd i ett arbetsavtalsförhållande. Enligt 36 a § 1 mom. i lagen om försvarsmakten (551/2007) får tjänster vid försvarsmakten tillsättas utan att de ledigförklaras. I paragrafens 2 mom. föreskrivs det om de tjänster som dock ledigförklaras.

Enligt 12 a § i polisförvaltningslagen får en sådan tjänst eller ett sådant tjänsteförhållande vid centralkriminalpolisen eller den lokala polisen som omfattar uppgifter inom användning av informationskällor, bevisprovokation genom köp, täckoperationer eller vittnesskydd, eller chefs- eller stöduppgifter som direkt anknyter till dessa uppgifter, tillsättas utan att tjänsten eller tjänsteförhållandet ledigförklaras, om uppgifternas art nödvändigt kräver det. Vid bedömningen av nödvändigheten ska hänsyn tas till 1) polisens personalsäkerhet och organisationsäkerhet, 2) uppgiften i fråga och de hot som är förknippade med den, 3) behovet av att skydda hemligt inhämtande av information eller 4) andra synnerligen viktiga allmänna eller enskilda intressen.

När en tjänst eller ett tjänsteförhållande som avses i 1 mom. tillsätts genom ett ansökningsförfarande, kan centralkriminalpolisen och lokalpolisen enligt 2 mom. låta bli att meddela dem som sökt tjänsten eller tjänsteförhållandet namnen på de andra sökandena och namnet på den som har utnämnts, om uppgiftens art nödvändigt kräver det på det sätt som avses i 1 mom. Sökandena ska dock underrättas om att tjänsten eller tjänsteförhållandet har tillsatts, och i utnämningsbeslutet ska nämnas den tjänst eller det tjänsteförhållande som tillsätts, vilken myndighet som har fattat beslutet samt datum för utnämningen.

Enligt 13 a § i polisförvaltningslagen får en tjänst eller ett tjänsteförhållande vid skyddspolisen tillsättas utan att tjänsten eller tjänsteförhållandet ledigförklaras, om uppgiftens art nödvändigt kräver det. Vid bedömningen av nödvändigheten ska hänsyn tas till 1) skyddspolisens personalsäkerhet och organisationssäkerhet, 2) uppgiften i fråga och de hot som är förknippade med den, 3) skyddet av den civila underrättelseinhämtningen eller 4) andra synnerligen viktiga allmänna eller enskilda intressen.

Enligt paragrafens 2 mom. ledigförklaras följande tjänster eller tjänsteförhållanden dock i enlighet med statstjänstemannalagen: biträdande chef, avdelningschef och enhetschef samt tjänster och tjänsteförhållanden som med hänsyn till uppgifterna är på motsvarande nivå.

När en tjänst eller ett tjänsteförhållande som avses i 1 mom. tillsätts genom ett ansökningsförfarande, kan skyddspolisen enligt 3 mom. låta bli att meddela dem som sökt

tjänsten eller tjänsteförhållandet namnen på de andra sökandena och namnet på den som har utnämnts, om uppgiftens art nödvändigt kräver det på det sätt som avses i 1 mom. Sökandena ska dock underrättas om att tjänsten eller tjänsteförhållandet har tillsatts, och i utnämningsbeslutet ska nämnas den tjänst eller det tjänsteförhållande som tillsatts, vilken myndighet som har fattat beslutet samt datum för utnämningen.

Med stöd av 15 j § i polisförvaltningslagen kan en tjänst som äldre konstapel, äldre kriminalkonstapel och yngre konstapel tillsättas utan att den förklaras ledig att sökas. När en tjänst tillsätts utan att den ledigförklaras får besvär inte anföras över tillsättningen. Ur skyddspolisens synvinkel är tjänsteförteckningar över tjänster som ska tillsättas utan att de ledigförklaras inte relevanta, och vid skyddspolisen används inte tjänstebeteckningarna äldre konstapel, äldre kriminalkonstapel och yngre konstapel eftersom uppgifterna skiljer sig från den övriga polisens uppgifter och behörighetsvillkoren kan vara restriktiva. Enligt 16 § i polisförvaltningsförordningen är behörighetsvillkor för äldre kriminalkonstaplar, äldre konstaplar och detektiver yrkeshögskoleexamen för polis, grundexamen för polis eller tjänsteexamen för polismanskap. Det rör sig om tjänster på manskapsnivå. Polisens verksamhet som avser bevisprovokation genom köp och täckoperationer samt uppgifter som gäller användning av informationskällor och vittnesskyddsprogram sköts i allmänhet av tjänstemän på minst underbefälsnivå, och därför lämpar sig bestämmelsen inte för rekryteringsförfarandet i fråga om tjänstemän som sköter sådana uppgifter.

Enligt 12 § 2 mom. i lagen om gränsbevakningsväsendets förvaltning (577/2005) får militära tjänster vid Gränsbevakningsväsendet tillsättas utan att de ledigförklaras. Enligt 9 § 1 mom. i lagen om Gränsbevakningsväsendets förvaltning finns vid gränsbevakningsväsendet följande militära tjänster: officer, specialofficer, institutofficer, sjöbevakare och gränsbevakare.

I utrikesförvaltningens karriärsystem avancerar de anställda efter den offentliga utlysningen under rekryteringen utan offentligt ansökningsförfarande. Enligt 15 § 1 mom. i lagen om utrikesförvaltningen (204/2000) tillsätts tjänsterna inom utrikesförvaltningen av statsrådet eller av utrikesministeriet enligt vad som bestäms genom förordning av statsrådet.

Enligt 2 mom. kan utrikesförvaltningens allmänna tjänster tillsättas utan att de ledigförklaras. En del av de allmänna tjänstemännen har med stöd av lagen skyldighet att övergå till ett annat uppdrag eller ett förflytta sig till ett annat tjänsteställe.

Offentlighetslagen tillämpas på rätten att få information och annat utlämnande av information ur en myndighets personregister. Utifrån principen om uppgiftsminimering i EU:s allmänna dataskyddsförordning konstateras det i finansministeriets anvisningar att det utnämningsbeslut som delges sökandena inte får innehålla personuppgifter om andra än den utnämnda personen, och det får innehålla endast motiveringen för valet av den personen. På processen vid tillsättningen av tjänster tillämpas sekretessgrunderna enligt offentlighetslagen, exempelvis lagens 24 § 1 mom. 29 punkt som gäller lämplighetsprov eller andra bedömningar eller lagens 24 § 1 mom. 31 punkt som gäller privata uppgifter. I samband med tillsättandet av en tjänst kan man också behöva ta hänsyn till offentlighetslagens 11 § som gäller partsoffentlighet, det vill säga en parts rätt att ta del av en handling även om den inte är offentlig, eller på ett bredare plan till den del som gäller den allmänna offentligheten (begäranden om information) behöva beakta sekretessgrunderna i lagens 24 §.

2.3 Bedömning av nuläget

2.3.1 Utlämnande av information om sabotageprogram

Det finns bestämmelser om utlämnande av information om sabotageprogram i 18 § 2 mom. och 74 § i lagen om militär underrättelseverksamhet. Den första av dessa är bunden till utvecklingen av metoderna och systemen för underrättelseinhämtning, det vill säga att det är möjligt att lämna ut uppgifter med utveckling av underrättelsemyndighetens verksamhet som utgångspunkt. Dessutom är utlämnandet av information bundet till nödvändighet.

I 74 § i lagen är utlämnandet av information bundet till den metod för underrättelseinhämtning med vilken informationen har fått. Således är det inte möjligt att lämna ut information om sabotageprogram vilken fått med andra metoder för underrättelseinhämtning till en aktör med ett behov av att få informationen.

Regleringen kan anses vara onödigt strikt med beaktande av den fortsatta digitaliseringen av samhället och den tekniska utvecklingen. Sabotageprogramaktörerna, framför allt APT-aktörer⁹, utgör inte något undantag till denna utveckling, utan de strävar efter att utveckla sin verksamhet ytterligare och snabbare än vad myndigheterna i målstaten och de privata aktörer som deltar i utvecklingen av datasäkerheten kan svara på. Således ska det vara möjligt att med en så låg tröskel som möjligt lämna ut information om sabotageprogram för försvaret av landet och för att skydda den nationella säkerheten.

Ett stort antal metoder för underrättelseinhämtning är tillgängliga för den militära underrättelseverksamheten. Uppgifter om sabotageprogram kan även fås med andra metoder för underrättelseinhämtning än underrättelseinhämtning som avser datatrafik, framför allt med metoder för underrättelseinhämtning som baserar sig på datatekniska metoder (till exempel teknisk observation av utrustning och underrättelseinhämtning som avser utländska datasystem). Således är det inte befogat att inhämta information om sabotageprogram uttryckligen genom underrättelseinhämtning som avser datatrafik.

I regleringen kring utlämnande av information om sabotageprogram ska man även beakta grundlagsutskottets ståndpunkt om att meddelanden som innehåller ett skadligt datorprogram eller kommando inte åtnjuter skyddet för hemligheten i fråga om förtroliga meddelanden enligt 10 § 2 mom. i grundlagen (GrUU 62/2024 rd, s. 4).

2.3.2 Installation och avinstallation av anordningar, metoder eller programvaror

Utifrån den gällande regleringen vidtas den åtgärd som beskrivs i paragrafen endast av en militärunderrättelsemyndighet. Vid underrättelseinhämtningen i praktiken har det dock observerats ett behov av att använda även aktörer som inte hör till en militärunderrättelsemyndighet för att vidta åtgärden. Detta gäller framför allt för effektiv utövning av befogenheten och förhindrande av att användningen av metoden för underrättelseinhämtning avslöjas. Om man även framöver förutsätter att endast en militärunderrättelsemyndighet kan vidta åtgärden, avgränsar detta åtgärden och användningen

⁹ APT är en förkortning av de engelskspråkiga orden Advanced Persistent Threat. Se skyddspolisens ”APT-operationer”, <https://supo.fi/apt-operaatiot>.

av den därpå följande metoden för underrättelseinhämtning på ett sätt som kan vara till skada för genomförandet av militärunderrättelsemyndighetens uppgifter.

I och med att tekniken utvecklats måste även militärunderrättelsemyndighetens verksamhet utvecklas för att förhindra att användningen av metoder för underrättelseinhämtning avslöjas. Vid underrättelseinhämtningen i praktiken har det observerats att effektivt vidtagande av den åtgärd som avses i paragrafen och användningen av metoden för underrättelseinhämtning kan förutsätta att en utomstående anordning eller datasystem används, för att militärunderrättelsemyndigheten ska ha åtkomst till det objekt som anknyter till åtgärden och användningen av metoden för underrättelseinhämtning. Utifrån den gällande regleringen är detta inte möjligt, varvid information som är behövlig för militärunderrättelsemyndighets uppdrag kan förbli dold.

2.3.3 Underrättelseinhämtning som avser datasystem i Finland

Så som lagts fram ovan i beskrivningen av nuläget, handlar de moderna datasystemen inte längre om enskilda anordningar och programvaror. Ett datasystem kan anses utgöras av 1) anordningar för informationsbehandling, anordningar för informationsöverföring, program som behandlar information och reglerna för behandling av information, 2) en geografiskt och logiskt utspridd helhet som består av flera olika anordningar och programvaror eller delar av sådana och 3) även delar som samtidigt hör till något annat datasystem.

Det är i sig möjligt att inhämta information från ovan beskrivna helhet, men det förutsätter att flera befogenheter utövas. Dessa befogenheter utgörs av teleavlyssning, teleövervakning, teknisk avlyssning och teknisk observation av utrustning.

Till exempel teknisk observation av utrustning identifierar inte ett ovan avsett datasystem i sin helhet. Om information inhämtas ur ett datasystem enligt kravet på riktad teknisk observation av utrustning, är det möjligt det blir svårt att inhämta information, det förhindras eller att det kräver en långt gående tolkning av lagen. Detta är fallet i synnerhet i situationer där inhämtandet av information inte riktar sig till en enskild anordning eller en programvara i den, till exempel till en helhet av flera internetserverar och flera programvaror. Sådana helheter utgörs av de flesta moderna system som är avsedda för utbyte av meddelanden och lagring av uppgifter och som ställts till förfogande för allmänheten eller som används av organisationerna. Användningen av teknisk observation av utrustning förutsätter att varje enskild anordning eller programvara identifieras och anges i ett yrkande på tillstånd för metoden för underrättelseinhämtning.

Identifiering av en anordning som en förutsättning för teknisk observation av utrustning enligt den nuvarande regleringen är problematisk i många av de situationer där information som ska inhämtas finns i en tjänst som är kopplad till ett datanät. I så fall kan anordningen identifieras endast med någon sekundär identifierare, vanligen med datanätets teleadress, till exempel IP-adressen.

Identifiering av en anordning och riktande av teknisk observation av utrustning ända till en anordning blir en problematisk fråga även om man har kännedom om anordningens existens och användning eller användare i och med information som inhämtats genom någon annan metod för underrättelseinhämtning, men det inte är möjligt att inhämta närmare identifieringsuppgifter med denna.

Bestämmelserna med definitioner av teleavlyssning och teleövervakning redogör för att dessa befogenheter tillämpas då inhämtandet av information hänför sig till ett meddelande som förmedlas i ett allmänt kommunikationsnät eller i ett kommunikationsnät som anslutits till det.

Det kan anses att det är nödvändigt att avskilja teleavlyssning och teleövervakning från området för teknisk avlyssning i huvudsak därför att dessa metoder, med avvikelse från det övriga inhämtandet av information som hänför sig till kommunikation, i regel måste genomföras med hjälp av kommunikationsförmedlaren (ett teleföretag), varför det funnits ett behov av att separat utfärda bestämmelser om skyldigheten för en kommunikationsförmedlare att bistå en myndighet i genomförandet av teleavlyssning och -övervakning.

Dessutom kan en tjänst som kommunicerar i en teleadress ha genomförts som en helhet med en anordning eller som en så kallad virtuell server, där en fysisk serverdator ansvarar för att köra flera program i en logisk virtualiserad dator och för att lagra uppgifterna. Därtill kan den anordning som är föremål för teknisk observation av utrustning vara placerad i datanätet på så sätt att kommunikationen med denna anordning sker via en kedja som består av flera anordningar för informationsbehandling och informationsöverföring. För att teknisk observation av utrustning av den anordning som är objekt för den egentliga underrättelseinhämtningen ska lyckas, måste man för att få den behövliga informationen även genomföra teknisk observation av utrustning av andra anordningar i kedjan.

I nuläget har den så kallade ända till ända-krypteringen ökat, vilket för egen del påverkat att tekniken används bland annat i de vanligaste kommunikationstjänsterna. Utbredningen av krypteringen har även lett till att man genom teleavlyssning inte alltid får tillräckligt omfattande information om objektets kommunikation, utan informationen om sända och mottagna meddelanden fås i praktiken från en anordning som utgör objekt. Även om teknisk observation av utrustning i sig delvis svarar mot detta problem i nuläget, ger den dock inte information i realtid på samma sätt som teleavlyssning. Å andra sidan är det inte nödvändigtvis möjligt att inhämta informationen ens med teleavlyssning, då informationen går via en kommunikationsapplikation.

Beskrivningen av nuläget redogör för att inhämtande av information om en och samma uppgift i en och samma datasystemhelhet är fragmenterad under flera olika befogenheter, beroende på om uppgiften vid tidpunkten för inhämtandet av informationen finns i en teknisk anordning, i ett allmänt kommunikationsnät eller i ett kommunikationsnät som anslutits till det eller i ett annat kommunikationsnät än ett allmänt kommunikationsnät eller ett nät som anslutits till det.

I fråga om underrättelseinhämtning som avser datasystem är det centrala problemet att det inte är möjligt att fullständigt gestalta ett datasystem i förväg. Det är möjligt att börja användningen av en metod för underrättelseinhämtning genom att rikta den mot en enskild anordning, såsom en terminalutrustning. Genom användningen av en metod för underrättelseinhämtning som riktas på terminalutrustning kan man få information om att terminalutrustningen eventuellt är i kontakt med en organisations centraliserade server. För att användningen av en metod för underrättelseinhämtning ska kunna riktas till exempel mot en server som används av en organisation, ska tillstånd först ansökas för teleavlyssning, för att få information om med vilken server terminalutrustningen står i kontakt. Därefter ska man på nytt ansöka om tillstånd till teknisk observation av utrustning för att kunna inhämta information från servern. Det faktum att de anordningar och programvaror som anknyter till ett datasystem och de metoder för underrättelseinhämtning som riktas mot dessa utgörs av en serie med flera delar leder till att det är svårt att få all information som behövs om verksamhet som allvarligt hotar landets försvar och den nationella säkerheten. Informationens snabba rörlighet är ett separat element.

Det ovan konstaterade leder att nuläget, i synnerhet i fråga om utredningar som gäller cyberspionage och -påverkan, inte anses vara fungerande, eftersom en enskild teknisk anordning som godkänts av en domstol som ett objekt för militär underrättelseinhämtning i praktiken alltid är en del av en helhet som omfattar tiotals eller till och med hundratals andra

anordningar, vilka den främmande staten utnyttjar i kedjelänkningen av sitt spionage mot Finland. Förbindelserna och kedjorna mellan anordningar som utnyttjas i fientligt sinnad statlig cyberverksamhet byggs upp och försvinner väldigt snabbt, varför domstolstillstånd för underrättelseinhämtning som hänför sig till dessa inte kan fås inom ramen för det tillgängliga tidsfönstret.

Lösningen är inte heller fungerande för underrättelseinhämtning som en militärunderrättelsemyndighet som riktar mot militär verksamhet och andra organisationer som utgör ett hot mot den nationella säkerheten och till och med för underrättelseinhämtning som hänför sig till enskilda personer. Så gott som utan undantag består moderna datasystem som är avsedda för digital kommunikation och behandling av data eller förvaring av data av anordningar och programvaror som opererar tillsammans (till exempel molnlagringsutrymmen som en enskild dator använder eller servrar som används i en viss organisationens e-postkorrespondens, datatrafikanordningar och kundprogram). På grund av detta kan teknisk observation av utrustning i dess nuvarande form inte anses vara fungerande.

I nuläget bildar den anordningsorienterade approachen ett problem till exempel i följande situationer:

- inhämtande av information som lagrats i olika molntjänster,
- andra sådana tjänster i vilka kommunikationen och interaktionen mellan användarna sker via en teledress, men tjänsten tillhandahålls av flera servrar i bakgrunden,
- en förfrågan som gäller cyberhotaktörers attackinfrastruktur och anonymiseringsnät vilka består av flera delar, som är kedjelänkade och geografiskt utspridda och som byggts på Internet,
- underrättelseinhämtning i utlandet där begränsningarna i verksamhetsmiljön minskar möjligheten för militärunderrättelsemyndigheten att identifiera den anordning i vilken den information som ska inhämtas lagras.

I fråga om de i detta sammanhang behandlade metoderna för underrättelseinhämtning finns det även skillnader i hur de riktar. Det är möjligt att yrka på att teleavlyssning, teleövervakning och teknisk avlyssning ska gälla en viss person och alla teleterminalutrustningar och teledresser som används av denna person, vilka innehas eller används av målpersonen under giltighetstiden för tillståndet. Beslutet om att enskilda teleterminalutrustningar eller -adresser omfattas av ett tillstånd som beviljats av en domstol fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Det motsvarande är inte möjligt i fråga om teknisk observation av utrustning. Dessutom är det inte möjligt att rikta teknisk observation av utrustning utifrån en teledress.

I fråga om informationssystemen kan det även uppstå situationer där inte står klart vilken metod för underrättelseinhämtning som ska användas. Detta är fallet exempelvis i en situation där en router som sammankopplar två servrar som en del av ett informationssystem eller en annan datatrafikförbindelse kan vara en del av ett allmänt kommunikationsnät eller så handlar det om ett internt nät i en organisation. Vid tidpunkten för själva inhämtandet av information står det inte nödvändigtvis klart om teleavlyssning eller teknisk avlyssning ska användas för att inhämta information om datatrafikförbindelsen. Å andra sidan kan man inte anse att teknisk avlyssning ursprungligen varit avsett för detta syfte, varvid endast avlyssning kan bli aktuellt, vars användning beror på om informationen rör sig i ett allmänt kommunikationsnät. I sista hand finns det i situationen inte någon metod för underrättelseinhämtning som kan användas på ett entydigt sätt.

2.3.4 Teknisk observation av utrustning

Enligt den gällande lagen kan teknisk observation av utrustning hänföra sig till en viss anordning eller programvara. Teknisk observation av utrustning har uttryckligen avgränsats även på så sätt att den kan hänföra sig till ett meddelande som förmedlas i ett kommunikationsnät och på vilket 34 § i lagen om militär underrättelseverksamhet tillämpas då inhämtandet av information riktar sig mot det. Således hänför sig teknisk observation av utrustning till användning av en anordning, en uppgift eller ett meddelande som lagrats i anordningen eller till en programvara som används i anordningen. För att teknisk observation av utrustning ska vara möjlig, förutsätter detta i praktiken att en anordning, metod eller programvara installeras i anordningen.

Mängden anordningar och programvaror ökar hela tiden. I synnerhet antalet terminalutrustningar och de abonnemang som används i dessa har på årsnivå ökat klart mer än antalet personer mot vilka underrättelsemetoder riktas. Dessutom har så kallad ända till ända-kryptering utbrejts i och med de kommunikationsapplikationer som är allmänt tillgängliga och som används allmänt, vilket för egen del försämrar möjligheterna att använda teleavlyssning.

Flera programvaror kan lagra information i en molntjänst till exempel som säkerhetskopior, utan att användaren själv kan påverka detta.

Enligt den gällande lagen kan inhämtande av information riktas på ett omfattande sätt mot de teleterminalutrustningar som innehas av föremålet och de teleadresser som föremålet använder i ett kommunikationsnät, till exempel genom att rikta teleavlyssning mot personen, men inhämtande av information kan inte riktas med motsvarande omfattning till själva anordningen eller de anordningar eller programvaror som personen använder.

Underrättelseinhämtning som görs i telenät omfattar inte exempelvis lagringsenheter, såsom hårddiskar och externa minnen, såsom USB-minnen. Dessutom kan man bedöma att utbudet av olika programvaror ökar i och med att den artificiella intelligensen utvecklas. Således kan föremålet för militär underrättelseinhämtning ha tillgång till ett stort antal teleterminalutrustningar och teleadresser och därtill andra lagringsanordningar samt programvaror som används i anordningarna. Riktande av inhämtande av information mot lagringsutrustning kan vara föremål för tidspress, eftersom informationen om lagringsutrustningen kan komma på ett överraskande sätt och möjligheten att installera en anordning, metod eller programvara i den kan likaså uppstå på ett överraskande sätt.

Redan för närvarande kan det i fråga om samma objekt vara nödvändigt att göra flera konsekutiva yrkanden och beslut i samma underrättelseuppdrag, ibland till och med varje vecka. Den gällande regleringens utrustnings- och abonnemangsspecifika karaktär föranleder således flera successiva berednings- och handlägningsprocesser i samma ärende både för förundersökningsmyndigheten och domstolarna. Den inskränkning i de grundläggande fri- och rättigheterna som teknisk observation av utrustning orsakar och som hänför sig till skyddet av konfidentiell kommunikation är av väsentlig vikt vid prövning som gäller teknisk observation av utrustning. Antalet anordningar eller programvaror som används av den person som är föremål för militär underrättelseinhämtning eller tillstånd till teknisk observation av utrustning vilka gäller dessa är inte av betydelse för detta. Det mer relevanta är däremot om det är möjligt att överhuvudtaget kränka skyddet för privatlivet eller skyddet för förtroliga meddelanden för en viss person som utgör föremål för militär underrättelseinhämtning genom teknisk observation av utrustning som riktas på en anordning eller programvara som han eller hon använder.

Dessutom kan det konstateras att teknisk observation av utrustning redan i praktiken är en metod som är av väldigt liknande typ eller åtminstone en metod som ligger väldigt nära teleavlyssning och teleövervakning, även om inhämtandet av information sker från en anordning och inte från ett elektroniskt meddelande som sänts från den eller som kommer till den.

Det verkar vara motiverat att regleringen kring teknisk observation av utrustning ändras så att den utöver anordningar och programvaror även är bunden till en person. I så fall innehåller tillståndet inte någon separat förteckning över alla anordningar eller programvaror, utan domstolen beviljar tillstånd att genomföra teknisk observation av utrustning i fråga om anordningar och programvaror som används av den person som är föremål för militär underrättelseinhämtning. Med anledning av ändringen behöver en militärunderrättelsemyndighet inte separat ansöka om enskilda tillstånd för varje anordning eller programvara som används av objektet och som klarnar efter beviljandet av tillståndet för teknisk observation av utrustning.

De anordningar som används kan för närvarande utredas genom inhämtande av information i ett telenät, inhämtande av identifieringsuppgifter om en teleterminalutrustning eller teleadress, personförfrågningar eller teknisk observation av utrustning. Anordningarna och programvarorna meddelas till domstolen i ansökan om teknisk observation av utrustning, och domstolen beviljar eller avslår tillståndet utifrån dessa uppgifter.

Utredningen av identifieringsuppgifter om de anordningar och programvaror som en person som utgör objekt för användning av en metod för underrättelseinhämtning använder förblir fortfarande ett ärende som en tjänsteman från militärunderrättelsemyndigheten ska utreda med tjänsteansvar. Samtidigt kunde motiveringsskyldigheten stärkas så att teknisk observation av utrustning endast riktas mot anordningar och programvaror som är nödvändiga med tanke på åtgärden. Detta skulle kunna säkerställas genom att förutsätta att en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman fattar ett separat beslut i ärendet, i vilket det motiveras varför föremålet för åtgärden utgörs av de valda teleadresserna eller teleterminalerna. Beslutet omfattas av laglighetsövervakningen, såsom underrättelsetillsynsombudsmannen.

Dessutom blir 85 § i lagförslag 1 relevant, vilken reglerar bland annat avbrytande av teknisk observation av utrustning, om den hänför sig till någon annan anordning eller programvara än en sådan som används av den person som är föremål för tillståndet.

2.3.5 Behandling av tekniska data om datatrafik

I den gällande lagen är behandling av tekniska data avsedd i synnerhet för identifiering av datatrafik från eller till ett visst geografiskt område eller en viss domän. Befogenheten är duglig och ändamålsenlig för identifiering av ett kommunikationsnätets del. Utifrån erfarenheterna från användningen av befogenheten har man observerat att den därtill ska kunna utövas även för den tekniska utvecklingen av underrättelseinhämtning som avser datatrafik. Det är ändamålsenligt att utvidga användningen av befogenheten på så sätt att den ger egentlig underrättelseinformation, såsom genom att kombinera uppgifterna med detaljerad information om underrättelseobjekten.

Befogenheten är därtill förknippad med kravet på tillfällig karaktär, som har preciserats i rättspraxis. Med beaktande av att man genom att använda befogenheten i praktiken inte får annan information än tekniska data om datatrafiken, kan kravet på tillfällig karaktär anses vara obefogat. Konstaterande av en tillfällig karaktär i praktiken, med beaktande av dess mål, kräver oproportionerligt mycket resurser och anses inte vara ändamålsenligt.

I behandlingen av tekniska data är det möjligt att det uppkommer information utifrån vilken det är möjligt att identifiera en enskild fysisk person, vilket innebär att de mottagna uppgifterna inte heller kan analyseras på ett sätt som sådan information kan producera. Således kan även intrånget i de grundläggande fri- och rättigheterna anses vara litet.

Utifrån den gällande regleringen kan information som fås vid behandling av tekniska data inte lagras för senare användning i militär underrättelseinhämtning. I den praktiska verksamheten har man observerat att de uppgifter som ligger i bakgrunden till den tekniska analysen kan vara till nytta även i den senare användningen av befogenheterna, där man kan utreda de aktörer som befinner sig i bakgrunden av datatrafiken och andra omständigheter. Det ska vara möjligt att använda information som fås vid behandling av tekniska data i de analyser som produceras i den egentliga underrättelseinhämtning som avser datatrafik och i fastställandet av nya sökbegrepp.

2.3.6 Sökbegreppen i underrättelseinhämtning som avser datatrafik

I 70 § i lagen om militär underrättelseverksamhet regleras underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer. Vid riksdagsbehandlingen av lagförslaget kompletterades paragrafens 1 mom. på så sätt att annan användning av underrättelseinhämtning än användning av underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer även förutsätter bland annat att de uppgifter som ska skaffas inte kan skaffas genom någon annan metod för underrättelseinhämtning. Eftersom tillämpningen av denna så kallade förutsättning om ett sistahandsalternativ redan i sig löser frågan om förhållandet mellan underrättelseinhämtning som avser datatrafik och metoderna för teleunderrättelseinhämtning (inklusive även andra metoder för underrättelseinhämtning), kan det separata ovillkorliga förbud som föreskrivits i 68 § 3 mom. och 70 § 2 mom. att som sökbegrepp använda en uppgift som identifierar en teleterminalutrustning eller teleadress som finns i Finland anses vara onödigt.

Dessutom förekommer det situationer där det är omöjligt att använda metoder för teleunderrättelseinhämtning, såsom teleavlyssning, men det är möjligt att använda en uppgift som identifierar en teleterminalutrustning eller teleadress som sökbegrepp för underrättelseinhämtning som avser datatrafik till den del som det är tillåtet. Till exempel en e-postadress är i fråga om juridisk natur en sådan teleadress som nämns i 68 § 3 mom. och 70 § 2 mom. i lagen om militär underrättelseverksamhet. Det är inte möjligt att rikta och genomföra teleavlyssning endast utifrån en uppgift som gäller en e-postadress, men enligt förslaget är det möjligt att använda information om en e-postadress som sökbegrepp i underrättelseinhämtning som avser datatrafik. I en situation där den aktör som använder en e-postadress förflyttar sig till finskt territorium, är det omöjligt att i förväg eller under förflyttningen styrka detta. Förbudet kan bli kritiskt, om föremålet förflyttar sig till Finland till exempel som en del av genomförandet av en militär plan. De uttryckliga förbuden i 68 § 3 mom. och 70 § 4 mom. i lagen att använda en teleadress som innehas av en person som vistas i Finland som sökbegrepp hindrar detta.

Å andra sidan kan inhämtande av information i en sådan situation även leda till en skyldighet att till och med utplåna information i en situation där informationen i sig fås på ett sätt som är förenligt med bestämmelserna, men informationen från första början inte hade fått inhämtas på grund av att föremålet kommit in på finskt territorium. Förbudet kan även leda till en situation där de aktörer som utgör föremål döljer sin verksamhet genom att använda VPN-tjänster och på så sätt visar att de är i Finland.

I förarbetena till lagen motiveras förbuden enligt 68 § 3 mom. och 70 § 2 mom. med ett behov av att minimera inverkan på utomståendes datatrafik. I praktiken har det visat sig att denna

motivering inte håller, eftersom det vid användning av information som identifierar en teleterminalutrustning eller teleadress som sökbegrepp vid underrättelseinhämtning som avser datatrafik är osannolikt att sökbegreppet träffar någon som är helt utomstående i trafiken. Information som identifierar en teleterminalutrustning eller teleadress kan anses vara det noggrannaste sökbegreppet, varvid utomståendes datatrafik inte når den automatiska behandlingen.

Förbudet att använda ett innehållsmässigt sökbegrepp kan inte anses vara ändamålsenligt med tanke på definitionen av sökbegrepp. Så som konstaterats i beskrivningen av nuläget, föreskrevs definitionen av sökbegrepp med riksdagens medverkan. I enlighet med definitionen avses med sökbegrepp en uppgift som används för att vid underrättelseinhämtning som avser datatrafik så avgränsat och exakt som möjligt i en del av kommunikationsnätet selektera den datatrafik som är föremål för underrättelseinhämtningen, varvid intrånget i skyddet för hemligheten i fråga om förtroliga meddelanden sker endast i den omfattning som är nödvändigt för att uppnå syftet med underrättelseinhämtningen.

I praktiken har det observerats att förbudet avsevärt försvagar ett effektivt riktande av underrättelseinhämtning som avser datatrafik och det kan, i motsats till lagstiftarens uttryckliga syfte, anses leda till situationer där underrättelsemyndigheten i onödan får tillträde till sådan kommunikation som är oväsentlig för det hot som är föremål för underrättelse och som kan åtnjuta skyddet för hemligheten i fråga om förtroliga meddelanden. I varje fall innehåller 84 och 86 § i lagen bestämmelser om militärunderrättelsemyndighetens skyldighet att utan dröjsmål utplåna uppgifter som skaffats genom underrättelseinhämtning som avser datatrafik. Genom utplåningsskyldigheten skyddas även framöver utomståendes kommunikation.

I många fall är det möjligt att formulera sökbegrepp som hänför sig till det semantiska innehållet i meddelanden på ett sådant sätt att de på ett bättre riktat sätt avskiljer datatrafik till den automatiska och manuella behandlingen vid underrättelseinhämtning som avser datatrafik än de nuvarande uttryckligen tillåtna sökbegreppen som gäller till exempel ID-adressdomäner, siffror som gäller autonoma system och domäner. Trots att kryptering har blivit vanligare, möjliggör användning av innehållet i ett meddelande som sökbegrepp att insamlingen blir precisare. I så fall är när inte, inte ens tillfälligt, sådana meddelanden som inte är relevanta med tanke på inhämtandet av underrättelseinformation underrättelsemyndigheternas analysystem.

Erfarenheterna har visat att de sökbegrepp som används redan för närvarande styr endast datatrafik som överensstämmer med sökbegreppet till underrättelsemyndighetens analysystem. I nuläget är det möjligt att i den närmare analysen dock behandla endast information vars tekniska data omfattar en uppgift som motsvarar sökbegreppet. Om en uppgift som motsvarar ett sökbegrepp hittas till exempel i e-posten i uppgifter som gäller en person som vidarebefordrat ett meddelande, kan informationen således inte analyseras mer ingående. Användningen av sökbegrepp som gäller innehållet skulle möjliggöra att även korrespondensen mellan vissa aktörer följs effektivare.

På det sätt som konstaterats i förarbetena till lagen om militär underrättelseverksamhet innehåller inte lagstiftningen i de europeiska kontrollstater som utfärdat bestämmelser om underrättelseinhämtning som avser datatrafik begränsningar eller hinder att använda innehållsmässiga sökbegrepp, utan de begränsningar som ställts på användningen av innehållsmässiga sökbegrepp kan anses vara en lösning som är säregen för Finland.

2.3.7 Ingripande i verksamheten i ett informationssystem som äventyrar landets försvar och den nationella säkerheten

Datasystemens och -nätens globala utbredning innebär en ny form av utmaning för avvärjandet av militära hot och hot mot den nationella säkerheten. Cyberhotaktörer och andra aktörer som hotar den nationella säkerheten, vilka i sin verksamhet drar nytta av datanät och -system, opererar i regel utomlands, men de kan längs datanäten påverka och spionera på finskt territorium och i datasystem som används av finska medborgare och organisationer.

I enlighet med Finlands ståndpunkt gäller den internationella rätten även i cyberverksamhetsmiljön. På grund av detta har Finland rätt att försvara sin suveränitet i cybermiljön och rätt att vidta åtgärder enligt den internationella rätten, med vilka fientliga åtgärder som riktar sig mot Finlands suveränitet och andra skadliga åtgärder kan förhindras.

Territorialövervakningslagen ger territorialövervakningsmyndigheterna en möjlighet att vidta behövliga åtgärder för att avvärja fientlig verksamhet, om den allvarligt och direkt äventyrar rikets säkerhet. Enligt 34 § 2 mom. 1 punkten i territorialövervakningslagen utgörs fientlig verksamhet av bland annat orättmätig militär verksamhet som en främmande stat eller en militär styrka utan beteckningar riktar mot finskt territorium eller som sker på finskt territorium.

Även om territorialövervakningslagens tillämpningsområde och befogenheter i sig kan lämpa sig även för cyberverksamhetsmiljön, fungerar lagen i praktiken inte i den – den gällande territorialövervakningslagen kan anses ha utfärdats för en fysisk verksamhetsmiljö, såsom land- och havsområdet och luftrummet. Dessa verksamhetsmiljöer är av avsevärt annorlunda natur än cyberverksamhetsmiljön, som i praktiken ägs helt av privata aktörer. Den reglering utifrån vilken det är möjligt att i cyberverksamhetsmiljön börja vidta åtgärder för att förhindra eller avbryta verksamhet som allvarligt äventyrar Finland ska således vara annorlunda.

I sig kan fientlig verksamhet enligt territorialövervakningslagen avvärjas även utanför finskt territorium, om det står klart att konsekvenserna tar sig i uttryck i Finland. Till exempel en missil som dirigerar sig mot Finland kan skjutas ner i det internationella havsområdet.

Dessutom innehåller 34 § 2 mom. 1 punkten, till vilken det hänvisats i lagen, en hänvisning till väpnad militär verksamhet. För närvarande har inte en enda stat konstaterat att den blivit föremål för väpnad militär verksamhet i cyberverksamhetsmiljön. I enlighet med den internationella rätten ska en cyberåtgärd som överskrider tröskeln för militära maktmedel dessutom orsaka allvarliga effekter för människornas liv eller hälsa eller fysiska skador. I situationer där ovan nämnda förutsättningar inte är uppfyllda, är det således inte heller möjligt att vidta åtgärder enligt territorialövervakningslagen.

Bestämmelsen om teleövervakning i polislagen innehåller inte något direkt ställningstagande till om det genom denna är möjligt att förhindra funktionen i en teleterminalutrustning eller en anordning som använder en teleadress, utan även utifrån specialmotiveringen ser det ut som om det snarare handlar om förhindrande av de elektromagnetiska vågor som behövs för att använda en teleterminalutrustning eller en teleadress. Således ser det ut som om befogenheten inte kan utövas för att förhindra till exempel datatrafik som kommer från en viss teleterminalutrustning och som rör sig i en viss fiberoptisk ledning eller för att myndigheten ska kunna stänga denna teleterminalutrustning via kommunikationsnäten, i synnerhet i en situation där aktören finns utanför Finlands gräns.

Bestämmelsens ordalydelse tar dock inte egentligen ställning till hur användningen av en teleterminalutrustning eller teleadress hindras. Förhindrandet är dock bundet till ett visst

område, vilket i enlighet med specialmotiveringen tyder uttryckligen på förhindrande av elektromagnetiska vågor.

I varje fall begränsas polisens och brottsbekämpningsmyndigheternas befogenhet till finskt territorium.

Med stöd av 62 § i lagen om militär underrättelseverksamhet har Försvarsmaktens underrättelsetjänst rätt till underrättelseinhämtning som avser utländska datasystem. Med stöd av befogenheten kan en militärunderrättelsemyndighet inhämta information från ett datasystem utanför Finlands gräns genom datatekniska metoder. På folkspråk kan metoden för underrättelseinhämtning kallas för hackning.

Bestämmelsen ger dock inte möjlighet att förhindra funktionen i ett datasystem i en situation där det datasystem som utgör föremål används till exempel för att lamslå verksamheten i Finlands vitala funktioner. En militärunderrättelsemyndighet kan således skaffa information om verksamheten i ett datasystem, men inte förhindra datasystemets skadliga verksamhet för Finland.

Försvarsmakten har möjlighet att ingripa i verksamhet i ett datasystem utanför Finlands gräns först i en situation där förutsättningarna för användning av militärt våld är uppfyllda. I den internationella rätten har väpnat våld i cybermiljön i allmänhet ansetts innebära att om följderna av en cyberattack motsvarar följderna av ett traditionellt väpnat angrepp, såsom död, allvarliga skador eller avsevärd fysisk förstörelse, kan det tolkas som väpnat våld på det sätt som avses i artikel 2(4) i FN-stadgan. Med tanke på suveräniteten har det ansetts att åtgärder som exempelvis leder till att en anordning eller programvara installeras på nytt kränker suveräniteten.

Påverkan via datanät och förhindrande av funktionen i de informationssystem som utgör objekt sker alltid i praktiken under tröskeln för väpnat våld, för att verksamheten enklare ska kunna bestridas och å andra sidan med medvetenhet om att målstaten inte kan vidta kraftigare åtgärder med anledning av påverkansåtgärdernas ”ringa karaktär”. I praktiken har inte en enda stat konstaterat att den blivit föremål för sådan cyberpåverkan som uppfyller tröskeln för väpnat våld.

På ovan konstaterade sätt kan en finländsk myndighet utanför Finlands gräns inte ingripa i ett akut hot eller ett hot som på befogade grunder potentiellt är allvarligt, även om objektet tydligt är ett visst informationssystem som används för att genomföra ett hot eller om ett visst informationssystem har observerats vara ett behövligt instrument för att genomföra hotet. Ingripande i verksamheten handlar i så fall om riktad påverkan över nätet av en anordning eller ett informationssystem, vilken har endast små eller inga konsekvenser överhuvudtaget för utomstående. Även om verksamheten påverkar funktionen i en anordning eller ett informationssystem som utgör objekt, kan det inte anses att det handlar om verksamhet som i fråga om konsekvenser jämföras med militärt eller väpnat våld, utan om en mindre motåtgärd som nödvändigtvis förutsätts för det egna skyddet och som hänför sig mot motpartens verksamhet eller om återställande av det lagliga tillståndet.

En separat fråga utgörs av så kallade lågintensiva cyberattacker och avancerade ihållande cyberhotsaktörer. I bägge fall är verksamheten inte punktmässig i den meningen att den slutar genom att enskild åtgärd avvärjs. Ovan beskrivna cyberhot förutsätter en ny form av approach i fråga om hur ett hot ska avvärjas. Den effektivaste avvärjningen är att verksamheten förhindras och skadas på ett sätt som leder till att hotaktören inte kan genomföra sin verksamhet.

I fråga om cyberverksamhetsmiljön ska man beakta på det höga tempot i miljön. Det första tecknet på ett dataintrång eller skadegörelse kan fås först i det skede då attackens mål har uppnåtts. I detta skede är det inte längre möjligt att vidta effektiva blockeringsåtgärder. För att det i praktiken ska vara möjligt att förhindra eller avbryta en cyberattack, ska man kunna vidta åtgärder till exempel i en kommandoserver för en cyberattack. Kommandoserverna finns i praktiken alltid utanför det finska territoriet.

En förutsättning för att effektivt svara på cyberhot är att det är möjligt att rikta åtgärder även på andra anordningar eller system än de som vid en viss tidpunkt orsakar ett konkret hot. Den infrastruktur som används i sabotageverksamhet är omfattande och komplex. Genom att påverka endast en anordning som direkt orsakar hot för Finland är det därför inte möjligt att påverka det hot som bildas av angriparen som helhet.

För att genomföra förebyggande åtgärder behövs en bedömning från militärunderrättelsen om det bästa sättet för att svara på hotet i fråga och mot vilken punkt i angriparens verksamhet åtgärden ska riktas för att åtgärderna ska vara så effektiva och proportionerliga som möjligt. Även om militärunderrättelsemyndigheten som enda myndighet har möjlighet att göra underrättelseinhämtning som avser datasystem utomlands, kan en finländsk myndighet med de nuvarande befogenheterna inte effektivt hindra cyberhot som riktas mot Finland från utsidan av det finska territoriet.

Flera stater drar även nytta av olika offentliga kanaler för att främja den egna agendan och sprida falska nyheter och desinformation som försvagar demokratin i målstaten, till exempel genom botnet eller med hjälp av artificiell intelligens. Det är inte möjligt att svara på verksamheten genom sedvanliga demokratiska metoder eller brottsbekämpningsmetoder. Om spridning av desinformation allvarligt hotar den nationella säkerheten, är det för närvarande inte möjligt att påverka den genom att störa eller förhindra verksamhet i anknytning till spridning av desinformationen genom att rikta åtgärder som förhindrar driften i system eller annan infrastruktur som används för detta.

I nuläget är det inte möjligt att vidta påverkansåtgärder exempelvis i en situation där Finland tydligt är ett objekt för en cyberhotaktör och verksamheten kan avslutas genom en åtgärd som vidtas mot aktörens infrastruktur. Infrastruktur och cyberattacker som genomförs genom att använda sådan eller förberedelse av sådana attacker kan inte störas eller aktivt förhindras i en situation där man till exempel i samband med en underrättelseoperation upptäcker att den utgör ett hot mot försvaret av landet eller mot den nationella säkerheten. I synnerhet avancerade ihållande cyberhotsaktörer använder en datanätsinfrastruktur med flera skikt, där infrastrukturen styrs via en kommandoserver. Det är möjligt att effektivare avvärja ett hot genom att hindra att kommandona från en kommandoserver når de lägre skikten, då cyberattacken aldrig når fram.

Den nuvarande regleringen hindrar även åtgärder för att störa verksamhet i sådana datasystem som används till stöd för mer sedvanliga hot i den fysiska världen eller så kallade hybridhot. Sådana datasystem kan vara till exempel kommunikationssystem som används av den aktör som ligger bakom hotet, logistiksystem eller datatekniska lösningar som är avsedda för systematisk statlig påverkan på sociala medier. Dessutom är det inte möjligt att ingripa i verksamheten i ett funktionsstyrningssystem med vilket man styr en drönarsvärm mot Finland, även om det är känt att drönarna är på väg mot Finland.

Cybermiljön har skapat en ny möjlighet för staterna att uppnå sina mål med nya metoder. Dessa mål kan vara bland annat att stärka den egna politiken och synen samt att försvaga demokratin i andra stater genom att påverka kritiska funktioner i samhället, såsom val, kritisk infrastruktur

eller informationsförmedlingen. Denna verksamhet beskrivs ofta med termerna hybridpåverkan eller omfattande påverkan.

Även om Finland i nuläget kan skydda sig mot försök till påverkan och svara på sådana på olika sätt, såsom genom att dra nytta av diplomati, införa sanktioner som en del av Europeiska unionen eller genomföra brottsundersökning, är dessa metoder inte tillräckliga för samtliga fall och det eftersträlvade slutresultatet uppnås inte med dessa. I dessa fall ska staten ha en möjlighet, det vill säga verktyg, för att genom lämpliga metoder direkt påverka sådan verksamhet som hotar staten.

En tydlig befogenhet, ett beslutssystem och en förmåga att svara på även andra än militära hot som hänför sig mot Finland i normala förhållanden är en väsentlig del av den nationella säkerheten och tryggandet av samhällets vitala funktioner. Flera västländer har en motsvarande befogenhet att svara på hot mot dem. Det internationella samarbetet som en del av alliansen (NATO) har en synnerligen stor betydelse för att avvärja hot. Framöver är det möjligt att det i alliansens referensram uppkommer kategorisering i förhållande till vilka medlemsländer som har befogenhet och förmåga att utöva påverkan i cyberversamhetsmiljön. En förutsättning för ett effektivt internationellt samarbete är en tydlig och fungerande nationell lagstiftning.

2.3.8 Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik

Det kan anses att 86 § i lagen om militär underrättelseverksamhet författningstekniskt sett är otydlig i en situation där information som inkommit till ett system för underrättelseinhämtning som avser datatrafik har utplånats utifrån 82 § 2 mom. eller 84 § 1 mom., det vill säga att det visat sig att informationen omfattas av underrättelseförbudet eller att informationen inte använts eller inte behövs i den militära underrättelseinhämtningen. I princip utplånas en uppgift ur ett system för underrättelseinhämtning som avser datatrafik direkt utifrån den grunden att uppgiften är omotiverad och inte behövs i den militära underrättelseinhämtningen.

I nuläget kan regleringen inte anses vara helt tydlig, med beaktande av 82 § 2 mom. och 84 § 1 mom. i lagen, vilka innehåller uttryckliga bestämmelser om uppgifter som ska utplånas utifrån den grunden att uppgiften är omotiverad. Dessutom innehåller 86 § i den nämnda lagen en separat hänvisning till ovan avsedda 82 § 2 mom.

Med beaktande av den författningstekniska otydligheten är det ändamålsenligt att ändra utplåningsregleringen i 86 § så att den motsvarar praxis, det vill säga att information som är onödig för landets försvar eller för att skydda den nationella säkerheten utplånas utan dröjsmål. Detta motsvarar vad som föreskrivs om utplåning av skyddspolisens uppgifter i 15 § i lagen om civil underrättelseinhämtning avseende datatrafik.

Utplåningsskyldigheten är av betydelse framför allt för underrättelseskyldigheten. Om uppgiften utplånas direkt, i regel automatiskt vid underrättelseinhämtning som avser datatrafik, har en militärunderrättelsemyndighet inte ens information utifrån vilken underrättelsen kan göras till den som blivit föremål för användning av en metod för underrättelseinhämtning.

2.3.9 Underrättelseskyldigheten

Underrättelse om metoder för underrättelseinhämtning som används i hemlighet av en myndighet är en väsentlig del av rättsskyddet. Med tanke på en individs rättsskydd är det viktigt att användningen av en hemlig metod för underrättelseinhämtning i princip ska underrättas till den som blivit föremål för användning av metoden. Om en individ inte får information om att

han eller hon varit föremål för hemlig underrättelseinhämtning, har han eller hon inte heller möjligheter att förvissa sig om att användningen av metoderna varit lagenlig. Individens möjlighet att utöva rättsskyddsmedel och få till exempel en ersättning för en lagstridig åtgärd kan då inte utövas.

Å andra sidan har det observerats att skyldigheten att göra en underrättelse även har en missbruksförebyggande betydelse och detta har ansetts vara till och med den huvudsakliga betydelsen med underrättelseskyldigheten. Underrättelsen är dessutom av betydelse med tanke på tillförlitligheten i användningen av metoder för underrättelseinhämtning. En sammanslutning har ett allmänt intresse att bevaka att metoder för underrättelseinhämtning används inom ramen för godtagbara gränser.

De ovan beskrivna mål som ställts för underrättelseskyldigheten kan dock uppnås på flera olika sätt.

I avgörandepraxis av Europeiska domstolen för mänskliga rättigheter (Europadomstolen) har underrättelser om användning av en metod för underrättelseinhämtning kopplats till att en individ har möjlighet att begära en prövning av om myndigheternas åtgärder varit lagenliga. Europadomstolen förutsätter dock inte att underrättelsen ska göras i alla situationer. Enligt den kan en underrättelse till varje objekt för en åtgärd äventyra de långsiktiga mål som låg till grund att man ursprungligen påbörjade underrättelseinhämtningen. Underrättelsen får inte heller avslöja underrättelsetjänstens arbetsmetoder, verksamhetsområde eller agenter.

Förebilden för 89 § i lagen om militär underrättelseverksamhet har i avsevärd grad utgjorts av underrättelse av hemligt inhämtande av information enligt 5 kap. i polislagen och 10 kap. i tvångsmedelslagen. I bägge fall anknyter inhämtandet av information uttryckligen till förhindrande i förväg, avslöjande och förundersökning av brott, vilka är åtgärder som har som syfte att tillgodose straffansvaret. Således kan en person som utgör objekt anses ha även ett accentuerat behov av att få information om hemliga myndighetsåtgärder mot honom eller henne redan med tanke på en rättvis rättegång. Underrättelseverksamhet hänför sig inte till kriminell verksamhet och underrättelseverksamhet har inte som mål att tillgodose straffansvaret. Exceptionellt kan användning av metoder för underrättelseinhämtning vara förknippat med tillgodoseande av straffansvaret i så kallade situationer enligt brandväggsregleringen i 79–80 § i lagen om militär underrättelseverksamhet. I dessa fall kan underrättelsen om användningen av metoder för underrättelseinhämtning i praktiken ske via partsoffentligheten för förundersökningsprotokoll.

Europadomstolens avgörandepraxis (framför allt i Centrum för Rättvisa-målet och innan dess avgörandet i till exempel Kennedy-målet) och de avsnitt som gäller den internationella jämförelsen (det sista gäller Sverige) redogör för att rätten till effektiva rättsskyddsmedel som skyddas i artikel 13 i Europakonventionen kan genomföras på många olika sätt. En underrättelse har inte ansetts vara av betydelse, om personerna och sammanslutningarna har rätt att få sin sak utredd med andra tillräckliga metoder och metoden inte är bunden till att göra en underrättelse. Lagen om övervakning av underrättelseverksamheten (121/2019) innehåller bestämmelser om en rätt för var och en som misstänker sig ha blivit föremål för användning av en metod för underrättelseinhämtning att överföra sitt ärende för prövning av underrättelsetillsynsombudsmannen. En person kan hänskjuta sitt ärende för att behandlas av underrättelsetillsynsombudsmannen, även om domstolen i fråga om användningen av metoden för underrättelseinhämtning fattat ett beslut om att ingen underrättelse om användningen av metoden för underrättelseinhämtning görs till den som blivit föremål för användningen.

Ombudsmannen har omfattande rättigheter att få information och därtill övervakar ombudsmannen verksamheten i förväg, i realtid och i efterskott. Ombudsmannen har även omfattande rättigheter att avbryta användning av en metod för underrättelseinhämtning och att överföra ärenden till förundersökning. En domstol, som vid handläggningen har en representation från underrättelsetillsynsombudsmannen, fattar beslut om de metoder för underrättelseinhämtning som innebär de mest betydelsefulla inträngen i integritetsskyddet.

Närmare granskat ser det ut som om 89 § 2 mom. i lagen innebär att underrättelseskyldigheten vid sidan om en eventuell målperson för underrättelseinhämtningen i väldigt omfattande grad hänför sig även till sådana personer som inte varit föremål för underrättelseinhämtningen, utan som av en eller annan orsak kommunicerar med föremålet för underrättelseinhämtningen eller som utgör egentliga utomstående med tanke på underrättelseuppdraget.

Underrättelseskyldigheten om i synnerhet användning av underrättelseinhämtning som avser datatrafik avviker i praktiken på avsevärt sätt från underrättelseskyldigheten avseende användningen av andra metoder för underrättelseinhämtning, vilken hänför sig endast till den person som nämnts som målperson för den ifrågavarande metoden för underrättelseinhämtning i yrkandet och beslutet. Den gällande underrättelseskyldigheten kan jämföras med att det finns en skyldighet att underrätta om systematisk observation även till alla personer som den tjänsteman som genomför observation har iakttagit under en observation som pågått i ett halvt år och om att optisk observation mot ett utrymme ska underrättas till alla personer som slumpmässigt och kortvarigt befunnit sig i det utrymme som är föremål den optiska observationen. I fråga om underrättelseinhämtning som avser datatrafik kan problemet dock upprepas tiotals gånger på grund av den mängd datatrafik som inkommer till ett system för underrättelseinhämtning som avser datatrafik.

Den gällande regleringen kan inte heller anses vara tydlig med tanke på tillämpningen. Förutsättningen för underrättelseskyldigheten avseende underrättelseinhämtning som avser datatrafik är att 1) personen befunnit sig i Finland vid den tidpunkt då underrättelseinhämtning som avser datatrafik riktat sig mot honom eller henne, 2) innehållet i hans eller hennes meddelande eller i information som han eller hon lagrat har utretts, 3) utredningen av ovan nämnda uppgifter har gjorts manuellt, 4) de utredda uppgifterna omfattas av området för ett förtroligt meddelande och 5) uppgifterna har inte utplånats.

Den komplicerade regleringen leder till svåra tolkningssituationer avseende till vem en underrättelse ska göras och vilka alla som omfattas av underrättelseskyldigheten vid den förhandenvarande tidpunkten. Regleringen förutsätter även att underrättelsemyndigheterna aktivt följer situationen och situationens utveckling bland annat i fråga om sådana identifieringsuppgifter som inte varit det egentliga föremålet för inhämtandet av information.

I enlighet med den gällande regleringen kring underrättelseinhämtning som avser datatrafik utgörs objektet för metoden för underrättelseinhämtning av datatrafik, i praktiken en viss organisations datatrafik. Således är syftet med användningen av metoden för underrättelseinhämtning inte att få information om en viss persons, utan en organisations verksamhet, såsom verksamheten vid en främmande stats väpnade styrkor eller en anknuten privat organisation. En enskild person är ofta inte av betydelse i praktiken.

Genom underrättelseinhämtning som avser datatrafik är det möjligt att man i väldigt omfattande grad får identifieringsuppgifter som gäller olika aktörers datatrafikförbindelser och det kan vara behövt att förvara dessa. Målen med underrättelseinhämtningen förutsätter dock inte nödvändigtvis att man utreder om en fysisk person ligger bakom varje identifieringsuppgift, vem den fysiska personen är eller om det meddelande som identifieringsuppgiften gäller åtnjuter

skyddet för hemligheten i fråga om förtroliga meddelanden. I extrema situationer verkar den gällande underrättelseskyldigheten leda till att underrättelsemyndigheten i fråga om onödiga uppgifter i praktiken genom andra metoder måste utreda identiteten på den som använt identifieringsuppgiften, varvid man ingriper i personens privatliv i onödan för personen själv, men även med tanke på underrättelseinhämtningen. I princip har en underrättelsemyndighet inte något behov av att utreda identiteten i en situation där en identifieringsuppgift som en person använder helt slumpmässigt nått ett system för underrättelseinhämtning som avser datatrafik.

Underrättelseskyldigheten enligt den gällande lagen kan även anses vara relativt omfattande med beaktande av lösningarna i de kontrolländer som lyfts fram i den internationella jämförelsen, såsom Norge och Sverige, och det som Europadomstolen i sin avgörandepraxis om underrättelseskyldigheten konstaterat om den övervakningshelhet som gäller för underrättelseverksamhet.

I praktiken har 89 § 6 mom. i lagen blivit central i fråga om underrättelseskyldigheten. Med stöd av det är det utifrån ett domstolsbeslut möjligt att avstå från att göra en underrättelse eller att skjuta upp den. Med beaktande av objekten för militär underrättelseinhämtning ansöks beslut om avstående från underrättelse ofta, i synnerhet om den verksamhet som är föremål för underrättelseinhämtning redan i liten mån kan vara förknippad med även andra än statliga aktörer.

Riksdagens justitieombudsman har i sin berättelse avseende år 2024 granskat tillståndsärenden som gäller metoder för underrättelseinhämtning vid Helsingfors tingsrätt. Enligt 5 a kap. 35 § i polislagen och 116 § i lagen om militär underrättelseverksamhet behandlas ett tillståndsärende som gäller en metod för underrättelseinhämtning vid Helsingfors tingsrätt. Vid granskningen framkom det bland annat att lagstiftarens avsikt i fråga om underrättelse om användningen av en metod för underrättelseinhämtning eventuellt inte genomförs på det avsedda sättet.

Med stöd av 89 § 8 mom. i lagen finns det inte någon skyldighet att göra en underrättelse till statliga aktörer. I praktiken fullgörs inte underrättelseskyldigheten och den var således inte heller av betydelse för personernas rättsskydd. Det kan anses att underrättelseskyldigheten och därmed rättsskyddet har fullgjorts via underrättelsetillsynsombudsmannen. Via ombudsmannens omfattande övervakning som täcker all underrättelseinhämtning kan det anses att rättsskyddet tillgodosetts även i mer omfattande grad än i fråga om en enskild person, eftersom ombudsmannen kan ingripa och i omfattande grad ingriper i eventuellt lagstridigt förfarande med sina omfattande befogenheter. Således kan det anses att ombudsmannen tillgodoser en persons rättsskydd även i fråga om dem som inte framför någon undersökningsbegäran.

En annan sak som påverkar fullgörandet av underrättelseskyldigheten är till vem en underrättelse ska göras, i synnerhet om de uppgifter som fås om en person är vaga och personens vistelseplats inte är känd. Att en person försvinner och vistelseorten blir oklar kan för egen del vara ett tecken på att personen på ändamålsenliga grunder varit objekt för underrättelseinhämtning. Det kan vara utmanande att fullgöra underrättelseskyldigheten i situationer där en person meddelat sina kontaktuppgifter till de behöriga myndigheternas register endast för att dölja sina verkliga avsikter. Användning av underrättelsemyndighetens resurser endast för att utreda personens identitet och vistelseort kan inte anses vara en ändamålsenlig användning av resurser.

Överlag kan det konstateras att regleringen om en underrättelse inte kan anses vara av stor betydelse för tillgödoseendet av rättsskyddet för en person med beaktande av underrättelsemyndighetens accentuerade behov av att hemlighålla verksamheten och å andra

sidan av det tillsynssystem som har många nivåer och som riktar sig mot underrättelsemyndigheterna. Dessutom kan regleringen, med beaktande av de mångformiga tolkningssituationerna, anses vara invecklad och oklar. En ansökan om utebliven underrättelse hos en domstol alltid då en metod för underrättelseinhämtning används leder även till en onödig administrativ börda för underrättelsemyndigheten och detta ökar även domstolarnas börda.

Underrättelsetillsynsombudsmannen kan även anses genomföra den förebyggande effekt som fastställts som ett mål för underrättelseskyldigheten. Om i praktiken vem som helst kan begära att ombudsmannen undersöker om den som framfört en begäran om undersökning blivit föremål för oerättigad underrättelseinhämtning av en underrättelsemyndighet, skulle detta utvidga gruppen av dem som framställer eventuell fortsatta juridiska åtgärder avsevärt jämfört med hur stor gruppen är endast med stöd av underrättelseskyldigheten. Detta bidrar till att styra en underrättelsemyndighet att förfara lagenligt och rikta sin verksamhet noggrant.

2.3.10 Deltagande i militär underrättelseinhämtning av en person som inte hör till en militärunderrättelsemyndighet

Deltagande av en annan myndighet

I 18 § i lagen om militär underrättelseverksamhet finns det bestämmelser främst om samarbetet och utbytet av information mellan myndigheter. Samarbetet kan inte anses täcka att en annan myndighet kan delta i den operativa verksamheten i underrättelseinhämtningen.

I synnerhet Gränsbevakningsväsendet har i fråga om sin befogenhet en central roll för militär underrättelseinhämtning i egenskap av bevakare av Finlands gränsområde. Till exempel i den nära framtiden kan gränsen mellan Finland och Ryssland öppnas till och med snabbt. Öppningen av gränsen kan orsaka en avsevärd uppgång i antalet passeringar av Finlands gräns, vilket ger en möjlighet för personer som vill skada Finlands säkerhet att enklare ta sig över gränsen som en del av en större grupp personer.

I synnerhet situationer som är överraskande för den militära underrättelseinhämtningen kan först komma till Gränsbevakningsväsendets kännedom, utan att Gränsbevakningsväsendet har någon möjlighet att vidta åtgärder till förmån för den militära underrättelseinhämtningen. I sådana situationer är det möjligt att man med tanke på den militära underrättelseinhämtningen identifierar till exempel att en person med största sannolikhet är kopplad till verksamhet som är föremål för militär underrättelseinhämtning. Det är inte tillräckligt att endast överföra informationen till en militärunderrättelsemyndighet, eftersom det på grund av situationens brådskande inte är möjligt att överföra den identifierade personen till systematisk observation som görs av en militärunderrättelsemyndighet.

Å andra sidan innehåller lagstiftningen, såsom lagen om militär disciplin och brottsbekämpning inom Försvarsmakten (89/2025), bestämmelser om en annan myndighets hjälp till Försvarsmakten. Lagens 187 § innehåller bestämmelser om bistånd av polisen, Gränsbevakningsväsendet och Tullen och samarbetet med dem. Bistånd enligt paragrafen handlar inte om handräckning, utan om att ifall huvudstaben inte har befogenhet för att utföra en åtgärd som är behövlig för att sköta en uppgift som gäller brottsbekämpning, kan polisen, Tullen eller Gränsbevakningsväsendet utifrån en begäran vidta en sådan enskild åtgärd som omfattas av dess befogenhet. Det finns inte någon motsvarande reglering i lagen om militär underrättelseverksamhet, varför Gränsbevakningsväsendet inte kan vidta assisterande åtgärder inom militär underrättelseverksamhet.

Uppdrag inom militär underrättelseinhämtning härrör sist och slutligen till en statlig aktör. Gränsbevakningsväsendets uppgifter är att upprätthålla gränssäkerheten och den inre säkerheten i staten samt den allmänna ordningen. Gränsbevakningsväsendets uppgifter kan anses vara sammanflätade med begreppet nationell säkerhet, men underrättelsemyndigheterna sköter inhämtandet av information i anknytning till den. Det kan konstateras att de faktiska föremålen för inhämtande av information inom militär underrättelseverksamhet är även en del av uppgifterna inom Gränsbevakningsväsendets inhämtande av information i egenskap av myndighet med ansvar för den nationella säkerheten. Det kan anses att riktade av åtgärder som gäller gränspasseringar till föremål för militär underrättelseinhämtning ofta motsvarar varandra eller åtminstone ligger väldigt nära varandra vid en gränspasseringssituation. Rätt för Gränsbevakningsväsendet att ge bistånd förutsätter att lagen om Gränsbevakningsväsendet ändras.

Om bestämmelser hade utfärdats om möjligheten för Gränsbevakningsväsendet att vidta enskilda åtgärder för en militärunderrättelsemyndighets räkning, skulle personen i ovan beskrivna exempel ha överförts till systematisk observation. Gränsbevakningsväsendet ska dock agera som en underordnad till militärunderrättelsemyndigheten när den vidtar åtgärder.

Deltagande av aktörer som står utanför myndigheterna i underrättelseverksamhet

I 42 § i lagen om militär underrättelseverksamhet finns det bestämmelser om installation och avinstallation av en anordning, metod eller programvara. En åtgärd med en koppling till utövning av den befogenhet som avses i paragrafen kan utföras av en tjänsteman som tjänstgör för en militärunderrättelsemyndighet. Således kan en annan aktör inte vidta åtgärder.

I 51 § i lagen om militär underrättelseverksamhet finns det bestämmelser om användning av informationskällor. Det väsentliga vid användning av informationskällor är att informationskällan har tillgång till de uppgifter som utnyttjas i verksamheten. Paragrafens 3 mom. innehåller ett uttryckligt förbud mot att uppgifter vid styrd användning av informationskällor kan ombes att inhämtas på ett sådant sätt som förutsätter utövning av myndighetsbefogenheter eller som äventyrar informationskällans eller någon annans liv eller hälsa.

I 2 kap. 17 § i polislagen finns det bestämmelser om situationer där en polis kan begära att en utomstående person i vissa situationer använder maktmedel för att utföra ett polisiärt uppdrag under polisens uppsikt. Dessutom finns det bestämmelser om lindrigare hjälp av en utomstående i 9 kap. 3 § i polislagen.

På ovan beskrivna sätt ger lagen om militär underrättelseverksamhet inte någon möjlighet att använda en person som inte hör till en militärunderrättelsemyndighet till exempel för att vidta en åtgärd som föreskrivs i 42 § i lagen om militär underrättelseverksamhet, även om detta kan vara det effektivaste med tanke på underrättelseverksamheten och detta å andra sidan kan minska behovet av styrd användning av informationskällor. I vissa situationer där en utomstående aktör kan installera eller avinstallera en anordning, metod eller programvara som en enskild åtgärd, är den fara för livet och hälsan som detta eventuellt orsakar därtill mindre för den biträdande personen jämfört med att personen måste användas inom ramen för styrd användning av informationskällor.

En militärunderrättelsemyndighet har en befogenhet att själv vidta dessa åtgärder, men i praktiken kan det vara omöjligt för en militärunderrättelsemyndighet att få möjlighet att vidta åtgärden. Med beaktande av de i polislagen föreskrivna möjligheterna för polisen att i sista hand

använda även externa personer för maktmedel, kan åtgärderna enligt 42 § i lagen om militär underrättelseverksamhet anses vara lindriga.

Även en myndighetsextern person kan frivilligt bistå en militärunderrättelsemyndighet. En person kan exempelvis tillfälligt överlåta sin bil för att användas av militärunderrättelsemyndigheten. Det är inte ändamålsenligt att utfärda separata bestämmelser om sedvanligt bistånd till en militärunderrättelsemyndighet, eftersom detta förfarande baserar sig på avtalsfriheten. Eftersom verksamheten inte föreskrivits hittills, har det å andra sidan inte varit möjligt att betala något arvode skattefritt och därmed har det inte varit möjligt att skydda biträdets liv och hälsa på bästa möjliga sätt.

I denna proposition föreslås att separata bestämmelser utfärdas om rätten för en myndighetsextern person att bland annat installera en programvara i en anordning hos den som är föremål för militär underrättelseinhämtning under styrning och övervakning av militärunderrättelsemyndigheten. På grund situationens natur kan den i sig anses ligga nära användning av informationskällor, varför även ett skattefritt arvode ska kunna betalas för den föreslagna nya verksamheten.

Ett arvode ska kunna betalas skattefritt till ovan beskrivna biträden på samma grund som i fråga om informationskällor. Arvodet ska i praktiken anses vara ringa. Detta leder även till att militärunderrättelsemyndigheten inte kan kringgå till exempel bestämmelserna om konkurrensutsättning och inte utifrån den övriga allmänna regleringen sträva efter att minimera till exempel de betalda skatterna.

Militärunderrättelsemyndigheten kan begära att en utomstående person tillhandahåller sedvanliga tjänster, såsom att en person med ansvar för underhållet av ett husbolag öppnar dörren till ett visst utrymme. Den person som gett bistånd i ärendet kan beläggas med yppandeförbud i enligt med 95 § i lagen. Regleringen ger dock inte någon direkt möjlighet att vidta åtgärder som av tradition hör till en myndighet, såsom att installera en anordning, metod eller programvara som möjliggör användning av en viss metod för underrättelseinhämtning.

Utländsk tjänsteman

I nuläget kan en utländsk tjänsteman fungera i biträdande uppgifter enligt vad som föreskrivits i 20 § 3 mom. i lagen om militär underrättelseverksamhet. De biträdande uppgifterna har avgränsats till vissa metoder för underrättelseinhämtning, vilka är 1) observation och systematisk observation, 2) förtäckt inhämtande av information, 3) täckoperationer, 4) bevisprovokation genom köp, 5) användning av informationskällor, 6) radiosignalspaning och 7) behandling av tekniska data. Metoderna för underrättelseinhämtning har avgränsats till de metoder som kan anses innebära ett litet ingrepp i de grundläggande fri- och rättigheterna och det är inte tillåtet att ingripa i hemligheten i fråga om förtroliga meddelanden med en endaste metod. Samarbetsverksamheten sker alltid inom ramen för militärunderrättelsemyndighetens bestämmanderätt och på dess ansvar.

Avgränsningen till endast vissa metoder för underrättelseinhämtning kan inte anses vara förenligt med syftet, eftersom till och med befogenheter som producerar nödvändig information lämnar utanför regleringen.

Dessutom orsakar biståndet tolkningsoklarheter i förhållande till hur intensivt en tjänstemannen för militärunderrättelsemyndigheten själv ska delta i användningen av en metod för

underrättelseinhämtning. Detta kan orsaka en risk för att verksamheten avslöjas och i sista hand att livet och hälsan äventyras.

I nuläget kan en utländsk tjänsteman inte delta till exempel i inhämtande av information i underrättelseinhämtning som avser datatrafik. Det står klart att en utländsk tjänsteman eller myndighet inte kan göra egna kopplingar till ett allmänt kommunikationsnät för underrättelseinhämtning som avser datatrafik, men deltagande i den tekniska och innehållsmässiga analysen av datatrafik, i synnerhet då krypteringen av datatrafik utbredd, ger ännu bättre riktad och bättre information för militärunderrättelsemyndigheten.

På motsvarande sätt har krypteringen av de olika kommunikationsapplikationerna utvecklats, varför teleavlyssning inte nödvändigtvis alltid ger den önskade information om innehållet i ett meddelande. Således betonas de metoder för underrättelseinhämtning där information hämtas från en terminalutrustning. I dessa situationer kan en utländsk tjänsteman ha det kunnande och den utrustning som behövs för att kunna inhämta informationen.

Till övriga delar kan regleringen kring internationellt samarbete anses vara fungerande. Beslutsfattandet, ansvaret och behörigheten ska fortfarande hör till militärunderrättelsemyndigheten.

2.3.11 Tryggande av informationskällor

Det kan vara utmanande att trygga säkerheten för en informationskälla vid operationer utomlands. I synnerhet i en situation där en informationskälla lämnat betydelsefulla uppgifter till den militära underrättelseverksamheten, ska informationskällan kunna tryggas. I vissa fall är det inte möjligt att trygga informationskällan i källans stationeringsland, varför det förnuftigaste är att få informationskällan till finskt territorium eller via finskt territorium till ett tredje land.

I 78 § 4 mom. i lagen om militär underrättelseverksamhet finns det en möjlighet för en militärunderrättelsemyndighet att bland annat ge en falsk handling till en informationskälla, om det är nödvändigt för att skydda källans liv eller hälsa. I alla situationer är det i praktiken dock inte möjligt att ge falska handlingar eller så är det i övrigt synnerligen farligt att exempelvis passera en gräns via ett officiellt gränsövergångsställe. Dessutom är det möjligt att man är tvungen att passera en gräns via ett gränsövergångsställe som i sig är officiellt, men på så sätt att gränsmyndigheterna inte känner till gränspasseringen.

I nuläget ser det ut som om att då militärunderrättelsemyndigheten hjälper en informationskälla med en okonventionell gränspassering, gör sig tjänstemannen vid militärunderrättelsemyndigheten skyldig till ett brott enligt 17 kap. 8 § i strafflagen. Till exempel under operationen för att rädda KGB:s dubbelagent Gordievski under Kalla kriget transporterades den centrala informationskällan utan gränsmyndigheternas kännedom via Finland till Norge och vidare till Förenade kungariket. Med tanke på den gällande strafflagen skulle de som hjälpt till med arrangemangen ha ställts inför straffansvar för att ha hjälpt dubbelagenten med olaglig inresa i landet.

I ovan beskrivna exempel, där Finland användes för transitering, hade informationskällan även gjort sig skyldig till riksgränsbrott enligt 17 kap 7 § i strafflagen, eftersom personen inte hade någon behörig handling då han passerade Finlands gräns. Om en informationskälla passerar Finlands gräns genom att använda handlingar enligt 78 § 4 mom. i lagen om militär underrättelseverksamhet, kan informationskällan därtill, om ärendet kommer fram, också göra sig skyldig till riksgränsbrott, eftersom handlingarna varit falska.

För att en finländsk underrättelsemyndighet ska kunna skapa förtroliga relationer till de allra viktigaste informationskällorna, kan det bedömas att trygghet av informationskällans säkerhet är en betydelsefull förutsättning för att skapa relationen och fördjupa den. En situation där en finländsk myndighet får avsevärda uppgifter från en informationskälla och lämnar informationskällan åt sitt öde efter att hans eller hennes liv eller hälsa äventyrats kan anses vara icke-önskvärd.

2.3.12 Platsspecifik underrättelseinhämtning och kopiering

Enligt 4 § i lagen om militär underrättelseverksamhet utgörs föremålen för militär underrättelseinhämtning av bland annat en främmande stats militära verksamhet och utländsk underrättelseinhämtning. Det är uppenbart att man till exempel i samband med platsspecifik underrättelseinhämtning som riktas mot militär underrättelseinhämtning av en främmande stat i Finland kan hitta sådana ämnen som eventuellt kan användas för att tillverka sprängmedel eller till exempel giftiga kemikalier. I allmänhet är det dock inte möjligt att enbart visuellt identifiera eller bedöma farligheten för sådana ämnen som hittats i samband med platsspecifik underrättelseinhämtning. I samband med till exempel platsspecifik underrättelseinhämtning som riktas mot en utländsk underrättelseaktör är det dessutom möjligt att man hittar sådana handlingar som kan förmodas innehålla skrifter som gjorts osynliga genom kemisk behandling eller andra åtgärder för att göra skriften hemlig.

I bägge ovan nämnda fall ska egendomen eller partiet kunna omhändertas för att möjliggöra en analys i laboratorieförhållanden och för att identifiera ämnet. I många fall är det möjligt att till exempel från ett ämne som misstänks vara råmaterial för ett sprängmedel eller toxin ta ett litet prov så att det med blotta ögat inte är möjligt att se att egendomen minskat. Även om det finns ett behov av att i sin helhet omhänderta ämnen, föremål eller egendom, är det åtminstone i en del fall uppenbarligen möjligt att byta dessa till sådana som utåt sett påminner om dem, men som är ofarliga, varvid den aktör som orsakar ett hot åtminstone inte direkt upptäcker omhändertagandet och risken för att avslöjas kan minimeras.

Befogenheten avseende omhändertagande och provtagning behövs till exempel för att förhindra en strävan om synnerligen allvarlig hybridpåverkan eller omfattande påverkan och för att möjliggöra förundersökning av förberedelse av anknutna brott, vilket föreskrivits som en straffbar gärning.

I 79–80 § i lagen om militär underrättelseverksamhet (den så kallade brandväggsparagrafen) föreskrivs de förutsättningar utifrån vilka en militärunderrättelsemyndighet har rätt eller skyldighet att till polisen anmäla ett brott som kommit fram med hjälp av användningen av en metod för underrättelseinhämtning. Redan i brandväggsregleringen har tröskeln för att anmäla ett brott som ägt rum bundits till uttrycket ”ett brott kan förmodas ha begåtts”, medan en anmälan om ett brott som kan förhindras förutsätter information om att ett brott är under planering. Enbart den omständigheten att man till exempel i samband med en platsgenomsökning hittar ett ämne, ett föremål eller egendom som inte kan identifieras, torde inte kunna ge upphov till en sådan förmodan om att ett brott ägt rum eller sådan information om att ett brott förbereds att det är möjligt att göra en brandväggsanmälan till polisen. Eftersom ärendet inte kan anmälas till polisen, ska militärunderrättelsemyndigheten kunna omhänderta ett ämne, egendom eller ett föremål för analys. Till den del som en analys visar att ett ämne, egendom eller ett föremål exempelvis uppenbarligen används för att begå ett brott, blir brandväggsregleringen tillämplig. Utifrån en mottagen brandväggsanmälan kan polisen vidta de åtgärder som är nödvändiga för att bekämpa ett brott och inleda förundersökningen av ett förberedelsebrott.

Det finns bestämmelser om beslut om platsspecifik underrättelseinhämtning i lagens 55 §, vars ordalydelse och motiveringar är motstridiga. Eftersom ett fordon är en plats till vilken man inte har allmänt tillträde under tidpunkten för platsspecifik underrättelseinhämtning, fattas beslut om detta i enlighet med bestämmelsen av en domstol, medan förarbetena till bestämmelsen (RP 203/2017 rd, s. 275) i sig entydigt tilldelar beslutanderätten till huvudstabens underrättelsechef eller en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman som förordnats uppdraget. Det står klart att ordalydelsen i lagen blir tillämplig.

Bakgrunden till motstridigheten är uppenbarligen att förebilden för befogenheten till platsspecifik underrättelseinhämtning varit befogenheten till platsgenomsökning, som regleras i 10 kap. i tvångsmedelslagen. Med avvikelse från definitionsbestämmelsen av platsspecifik underrättelseinhämtning nämns riktande av platsgenomsökning mot ett fordon separat i definitionsbestämmelsen avseende platsgenomsökning i 10 kap. 1 § 4 mom. i tvångsmedelslagen. Enligt den avses med platsgenomsökning genomsökning av andra platser än sådana som avses i 2 eller 3 mom. trots att de inte är allmänt tillgängliga eller den allmänna tillgängligheten har begränsats eller hindrats vid tidpunkten för genomsökningen, eller genomsökning av ett fordon. Enligt 15 § 1 mom. i tvångsmedelslagen fattas beslut om platsgenomsökning av en anhållningsberättigad tjänsteman.

Det ovan beskrivna medför osäkerhet i fråga om platsgenomsökning av ett fordon och beslut om sådan. Det finns skäl att utfärda bestämmelser om platsspecifik underrättelseinhämtning som hänför sig till ett fordon som en egen undervariant av platsspecifik underrättelseinhämtning och på motsvarande sätt är det befogat att på samma sätt som i tvångsmedelslagen i fråga om platsgenomsökning tilldela beslutsfattandet till den organisatoriskt ansvariga nivån, det vill säga till en med användning av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

2.3.13 En militärunderrättelsemyndighets rätt att få uppgifter

Med stöd av 17 § i lagen om Försvarsmakten kan en militärunderrättelsemyndighet få ett lagstadgat uppdrag från en myndighet eller en sammanslutning som inrättats för att sköta en offentlig uppgift. Bestämmelsen kompletterar vad som föreskrivits i 37 § i lagen om behandling av personuppgifter inom Försvarsmakten.

I fråga om polisen, med undantag för skyddspolisen, har det ansetts att bestämmelserna om de centrala uppgifterna i en fullgöranderapport är specialreglering i förhållande till polisens allmänna rätt att få information. Rätten att lämna ut uppgifter gäller uttryckligen för uppgifter som är nödvändiga för att utreda och väcka åtal i brott. Eftersom utlämnandet av uppgifter har avgränsats för polisen i specialregleringen, har det inte varit möjligt att lämna ut information till skyddspolisen till exempel för att skydda den nationella säkerheten. På grund av detta har det varit nödvändigt att utfärda separata bestämmelser om rätten att lämna ut uppgifter till skyddspolisen.

Eftersom rätten att få uppgifter för Försvarsmakten inte begränsats på ovan beskrivna sätt i speciallagstiftningen, har militärunderrättelsemyndigheten med stöd av 17 § i lagen om försvarsmakten rätt att få uppgifter i motsvarande omfattning som skyddspolisen.

Det ovan konstaterade ger dock inte militärunderrättelsemyndigheten rätt att få en fullgöranderapport enligt lagen om Enheten för utredning av gård ekonomi, vilken ska föreskrivas uttryckligen i 6 § i lagen.

2.3.14 Inhämtande av information från allmänt tillgängliga källor

Behovet av information som inhämtats från öppna källor är större vid Försvarsmakten än i brottsbekämpningen och underrättelseverksamheten. Öppna källor erbjuder till och med avsevärd information till exempel för Försvarsmaktens undersökningsverksamhet och cyberförsvar. Så som i övrigt i Försvarsmaktens verksamhet, är det möjligt att inhämtandet av information är förknippat med ett behov av att dölja tjänstemannen och bakgrundsorganisationen.

Ofta kan information från öppna källor i sig vara offentlig, men det kan förutsättas att informationen skaffas på dolt sätt. I vissa fall kan till exempel begäran om information som framförts elektroniskt till en myndighet förutsätta att en svarsadress meddelas, vilket med tanke på Försvarsmaktens verksamhet och tillgång till information inte alltid kan vara en adress som kan kopplas till Försvarsmakten. Således ska det vara möjligt att för underrättelseinhämtning från allmänt tillgängliga källor använda även lätta täckidentiteter för att skydda underrättelseinhämtningen.

I och med att tjänsterna utvecklas delas information allt oftare i olika applikationers och meddelandeapplikationers grupper. I sig kan grupperna vara öppna och godkännandet till dem sker automatiskt eller utan att en person som vill ansluta sig till den utreds desto mer. Grupperna kan ha tusentals, hundratusentals och till och med miljoner medlemmar. Således kan en grupp i praktiken hållas öppen. Ofta förutsätts att man registrerar sig till den applikation som används för att kunna ansluta sig till en grupp, vilket även kan avslöja information om ställningen för den som inhämtar information och det verkliga ändamålen för underrättelseinhämtningen.

Den stora mängden information i allmänt tillgängliga källor medför utmaningar för behandlingen av den. I synnerhet i ett allmänt datanät finns det en enorm mängd information och det karakteristiska för informationen i ett sådant är, utöver den stora mängden, även att informationen uppdateras eller raderas snabbt. Det är mödosamt och långsamt att samla in information manuellt och det är möjligt att viktig information inte fås, eftersom informationen raderas snabbt till exempel från en grupp och en kanal i en direktmeddelandetjänst.

Övervakningen av underrättelseinhämtning som hänför sig till allmänt tillgängliga källor och lagringen av uppgifter har även i viss mån förblivit öppna frågor då verksamheten är underkastad sedvanerätt. I synnerhet den tekniska utvecklingen och uppgången i mängden uppgifter i allmänt tillgängliga källor har lett till att korsvis analys av den stora informationsmängden och information som inhämtats från olika allmänt tillgängliga källor med avancerad informationsbehandling eller med artificiell intelligens kan avslöja avsevärda uppgifter om personer och målverksamheten. Eftersom det inte finns särskild reglering för utplåning av information, kan obehandlad information därtill under årens och årtiondenas lopp ansamlas i avsevärda mängder, vilket inte heller ur myndighetsverksamhetens synvinkel kan anses vara ändamålsenligt.

I och med den tekniska utvecklingen har även fientlig cyberverksamhet och dataintrången ökat avsevärt. I vissa fall delas den informationsmassa som skaffats i verksamheten allmänt till exempel i ett dolt nät (såsom nätet Tor). I nuläget, som baserar sig på sedvanerätten, står det inte helt klart om någon annan än den behöriga brottsbekämpningsmyndigheten kan skaffa informationsmassa som skaffats i samband med ett brott åt sig själv. Informationsmassorna kan innehålla synnerligen viktig information till exempel med tanke på Försvarsmaktens beredskap, undersökningsverksamhet och cyberförsvar. I fråga om ovan beskrivna informationsmaterial kan myndighetens inhämtande av information vara förenligt med något brottsrekvisit.

Eftersom Försvarmakten är en stor organisation, kan det nuvarande inhämtandet av information som baserar sig på sedvanerätten genomföras av alla förvaltningsenheter vid Försvarmakten. Förutsättningen för inloggning i olika tjänster är att skapa en pseudonym och för närvarande kan laglighetsgrunden för användningen av en sådan och dess övervakning anses vara oklar, varför det finns ett behov av reglering.

Inhämtande av information från allmänt tillgängliga källor (letande och insamling av information) förutsätter inte alltid behandling av personuppgifter. Om man dock behandlar personuppgifter, så ska myndigheten vid inhämtande av information från allmänt tillgängliga källor beakta även lagstiftningen kring behandlingen av personuppgifter. Personuppgifter utgörs av alla uppgifter som anknyter till en identifierad eller identifierbar fysisk person. Personuppgifter omfattar till exempel namn, telefonnummer, positionsuppgifter och pseudonymer. I fråga om behandlingen av personuppgifter kan regleringen anses vara tydlig, eftersom behandlingen av personuppgifter inom Försvarmakten regleras i lagen om behandling av personuppgifter inom Försvarmakten.

2.3.15 Rekryteringen vid Försvarmakten

Med tanke på inhämtande av kunnande har Försvarmakten å ena sidan ett behov av att utnyttja det normala offentliga ansökningsförfarandet, men å andra sidan orsakar förfarandet ett operativt problem och ett arbetssäkerhetsproblem i vissa situationer. Med tanke på behovet av kunnande bör rekryteringen av personal kunna genomföras i ett öppet förfarande, samtidigt som man möjliggör ett icke-offentligt förfarande. Med tanke på vissa uppgifter vid Försvarmakten är det problematiskt att namnen på dem som sökt och utnämnts till en tjänst är offentliga. Verksamhet som stör Försvarmaktens arbete och som bedrivs av aktörer från främmande stater är långsiktig och pågår i flera år, varvid en möjlighet att sammanställa namnlistor och inhämta noggrannare uppgifter från handlingarna utgör en risk. Tryggande av liv och hälsa för de personer som deltar i verksamheten och i och med det skyddet av till exempel metoderna för underrättelseinhämtning och dess struktur börjar från det att rekryteringen startas.

Det är möjligt att skapa namnlistor som gäller Försvarmaktens verksamhet och personal, eftersom en ledigförklarad tjänst och namnet på dem som sökt en visstidstjänst är offentliga, ämbetsverken har en skyldighet att meddela namnet på den valda personen. Därtill ges uppgifter om utnämningsbeslutet och dess motiveringar med tanke på ändringssökande. Insändningen av en ansökan till en ledigförklarad uppgift kan inte avgränsas, utan alla ansökningar som inkommit inom den utsatta tiden och även därefter behandlas i processen för att tillsätta en tjänst. Då har sökandena partsställning och därmed rätt att överklaga beslutet om tillsättning av tjänsten. För besvärprocessen ska en sökande enligt finansministeriets anvisningar om tillsättning av tjänster på begäran ges en förteckning över de övriga sökandena samt utnämningsspromemorian och meritsammandraget. Ovan nämnda handlingar innehåller information som är mer omfattande än enbart namnet.

För närvarande är lagstiftningen kring Försvarmakten asymmetrisk i förhållande till lagstiftningen kring polismyndigheterna och de civila underrättelsemyndigheterna. Regleringen kring rekryteringsförfarandena borde harmoniseras för att vara likadan som rekryteringsregleringen för övriga säkerhetsmyndigheter, eftersom de offentliga intressena bakom regleringen kan anses vara jämförbara. Regleringen kring Försvarmakten har fungerat på ändamålsenligt sätt, men i den förändrade säkerhetsmiljön har man observerat underrättelseinhämtning som görs via rekryteringsprocesserna. Genom regleringen i polisförvaltningslagen har man kunnat svara på dessa utmaningar och därtill kan regleringen i fråga om det offentliga intresset jämföras även med rekryteringsregleringen för de övriga säkerhetsmyndigheterna.

3 Målsättning

Målet med propositionen är att uppdatera lagen om militär underrättelseverksamhet, som trädde i kraft som en ny lag år 2019, i enlighet med föresatserna i regeringsprogrammet och de behov som observerats i den praktiska tillämpningen. Målet är att möjliggöra och trygga en ändamålsenlig och effektiv verksamhet för militärunderrättelsemyndigheterna både nationellt och som en del av alliansen.

Målet är att upprätthålla och förbättra den nationella säkerheten, då man på ett ännu noggrannare och riktat sätt får information om målen för militär underrättelseinhämtning och då analyserad information kan delas ännu bättre till dem som behöver sådan. Förmågan hos militärunderrättelsemyndigheten att samla in information från objekten för militär underrättelseinhämtning förbättras genom att möjliggöra att olika aktörer får möjlighet att lämna ut vissa uppgifter till militärunderrättelsemyndigheten trots sekretessbestämmelserna. I fråga om underrättelseinhämtning som avser datatrafik förbättrar propositionen dessutom skyddet för hemligheten i fråga om ett privat meddelande genom att på samma gång dock förbättra inhämtandet av information för militär underrättelseinhämtning.

Ett ytterligare mål är att ge Gränsbevakningsväsendet en möjlighet att stödja en militärunderrättelsemyndighet i vissa avgränsade situationer och att förtydliga rollen för Armén, Marinen och Flygvapnet vid militär underrättelseinhämtning.

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

Installation och avinstallation av anordningar, metoder eller programvaror

Till 42 § i lagen om militär underrättelseverksamhet fogas ett nytt 2 mom., enligt vilket en person utanför militärunderrättelsemyndigheten får vidta en åtgärd enligt 1 mom. i paragrafen. I nuläget är åtgärderna möjliga för en militärunderrättelsemyndighet.

Den som vidtar åtgärden ska förfara noggrant enligt myndighetens anvisningar. På motsvarande sätt får de anvisningar som en myndighet gett inte lämna prövningsrätt för den som vidtar åtgärden i fråga om vidtagandet av åtgärden. Eftersom den som vidtar åtgärden inte har självständig prövningsrätt i fråga om åtgärden, förfar han eller hon till denna del under myndighetens behörighet. Således ansvarar militärunderrättelsemyndigheten även för eventuella skador som orsakas i enlighet med bestämmelserna i 4 kap. i skadeståndslagen (412/1974). Vid eventuella skadestånd handlar det om en motsvarande situation som om myndigheten själv hade gjort installationen och detta hade orsakat oförutsedda skador på installationsobjektet.

Om den som vidtar åtgärden inte iakttar de anvisningar som getts till honom eller henne och förfar utanför anvisningarna, ansvarar den som vidtagit åtgärderna personligen för de förorsakade skadorna. Till denna del kan skadeståndsansvaret anses jämföras med att en styrd informationskälla på egen hand vidtar andra åtgärder utanför de anvisningar som myndigheten gett honom eller henne.

Det föreslås att ett nytt 3 mom. fogas till paragrafen. Enligt det kan en militärunderrättelsemyndighet göra en installation eller avinstallation enligt paragrafens 1 mom. genom att använda även en extern anordning eller ett externt informationssystem. Redan för

närvarande kan 42 § anses ge möjlighet till detta, eftersom bestämmelsen inte tar ställning exempelvis till hur skyddet för informationssystemet kan kringgå. I den nya bestämmelsen konstateras uttryckligen att detta är möjligt.

Även i detta fall betonas i fråga om åtgärden riskbedömningen av att åtgärden inte orsakar någon skada för en utomstående och noggrann planering av åtgärderna.

Underrättelseinhämtning som avser datasystem mot en statlig aktör i Finland

Det föreslås att 4 kap. i lagen om militär underrättelseverksamhet innehåller bestämmelser om en ny befogenhet till underrättelseinhämtning som avser datasystem, med vilken det genom datatekniska metoder är möjligt att skaffa information om verksamheten i ett datasystem som utnyttjas för militär verksamhet eller för att allvarligt hota den nationella säkerheten, de uppgifter som det innehåller, meddelanden som rör sig mellan datasystemets delar och om meddelanden som inkommer till eller avgår från datasystemet.

Med datasystem avses en helhet som utgörs av anordningar för informationsbehandling, anordningar för informationsöverföring, program som behandlar information och protokoll för behandling av uppgifter. Ett datasystem kan utgöras av en geografiskt och logiskt utspridd helhet som består av flera olika anordningar och programvaror eller delar av sådana. Datasystemet kan täcka delar som samtidigt hör till något annat informationssystem. Underrättelseinhämtning som avser datasystem hänför sig till den logiska helhet som bildas av anordningar och virtuella system som kommunicerar sinsemellan i ett visst syfte som hotar den nationella säkerheten eller i ett visst militärt syfte, varvid inget tillstånd förutsätts separat för varje sådan anordning som hör till helheten.

Genom underrättelseinhämtning som avser datasystem är det möjligt att inhämta information antingen från hela datasystemet eller från en viss logisk eller fysisk del av ett datasystem, vilken genomför någon funktionalitet i datasystemet eller som i övrigt kan fastställas som en egen del av datasystemet baserat på datasystemets användare eller på uppgiftsinnehåll som på befogade grunder finns i datasystemets del.

Bland de gällande befogenheterna kan underrättelseinhämtning som avser datatrafik i Finland som helhet anses täcka bland annat teleavlyssning och teknisk observation av utrustning. På grund av detta ska beslutet om sådan fattas av en domstol. Det tillstånd som beviljats av en domstol ska gälla ett datasystem, varvid en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman ska fatta beslut om en enskild teleadress, en anordning för informationsbehandling, en anordning för informationsöverföring eller ett program för informationsbehandling och behandlingsprotokollet för data hör till det datasystem som utgör objekt. Besluten ska vara motiverade och laglighetsövervakning ska hänföras till dessa.

I ett yrkande eller ett beslut som gäller underrättelseinhämtning som avser datasystem i Finland ska man vid sidan om övriga omständigheter redogöra för avgränsningen av det datasystem som är föremål för åtgärden utifrån en beskrivning av datasystemets funktion, dess protokoll för informationsbehandling, identifierarna för de anordningar eller program som hör till det, de teleadresser som det använder, dess användares teleadresser eller andra användaruppgifter eller en kombination av några av dessa uppgifter på så sätt att inhämtandet av information kan avgränsas tekniskt sett utifrån beskrivningen.

De lagstadgade avlyssningsförbuden utsträcks till att gälla även underrättelseinhämtning som gäller inhemska datasystem på samma sätt som de i nuläget gäller teleavlyssning och anskaffning av uppgifter i stället för sådana, teknisk avlyssning och teknisk observation av utrustning.

Det föreslås att 42 § i lagen (installation av en anordning, metod eller programvara) utvidgas till att gälla även underrättelseinhämtning som avser datatrafik i Finland.

Ingripande i verksamheten i ett datasystem som äventyrar landets försvar och den nationella säkerheten

Till 62 § i lagen om militär underrättelseverksamhet fogas ett nytt moment. Enligt momentet har militärunderrättelsemyndigheterna rätt att vidta åtgärder i ett datasystem utanför Finlands gräns med vilka det är möjligt att genom datatekniska metoder hindra användningen av ett datasystem utanför finskt territorium, eller störa eller ändra dess funktion, om det genom datasystemet eller med hjälp av det är möjligt att orsaka allvarlig fara för Finlands försvar eller nationella säkerhet.

I den nuvarande cyberhotsmiljön har tydliga cyberattacker som uppfyller förutsättningarna för väpnade maktmedel och militär maktmedel inte ägt rum eller åtminstone har man inte identifierat att sådana ägt rum. Lågintensiva cyberattacker och avancerade ihållande cyberhot har däremot blivit betydande cyberhot. Deras betydelse beror på att bekämpning av en enskild åtgärd inte räcker för att stoppa verksamheten av den som utgör ett hot. Det är möjligt att effektivare ingripa i verksamheten genom åtgärder som hindrar eller skadar funktionen för infrastrukturen för den aktör som utgör ett hot i syfte att förhindra att hotet blir verklighet.

I den militära verksamhetsmiljön som för närvarande utvecklas i snabb takt är den militära verksamheten på motsvarande sätt i tilltagande grad beroende av datatrafikförbindelser och olika system för att styra anordningar och utrustningar. I en situation där exempelvis en drönarattack riktas mot Finland, kan hotet avvärjas på det effektivaste sättet genom att vidta åtgärder i styrningssystemet, vilka hindrar drönarna för att styras till finskt territorium eller att drönare överhuvudtaget sänds.

Det är ändamålsenligt att tilldela vidtagandet av förhindrande och skadande åtgärder till en militärunderrättelsemyndighet, som redan för närvarande har möjlighet att använda underrättelseinhämtning som avser datasystem i utlandet i objektet.

Åtgärderna ska vara förenliga med internationell rätt, proportionella och tillfälliga. En förutsättning för att vidta åtgärderna är att beakta utrikes- och säkerhetspolitiska ståndpunkter, som beaktas via ett i 15 § i lagen om militär underrättelseverksamhet avsett gemensamt möte om utrikes- och säkerhetspolitiken för utrikes- och säkerhetspolitiska ministerutskottet och republikens president.

En militärunderrättelsemyndighet är den enda myndighet som har befogenhet att inhämta information från ett datasystem som finns utomlands. Således har militärunderrättelsemyndigheten en uppfattning av vilken aktörs system det handlar om och när man med systemet eller via det orsakar en allvarlig fara för Finlands landsförsvar eller nationella säkerhet. Ett utländskt datasystem utgör planmässig verksamhet som förutsätter långvariga och diskreta förberedelser. Således kan det med tanke på resursfördelningen och den tillgängliga tiden inte anses vara förnuftigt att en annan myndighet i dessa situationer vidtar åtgärder för att genomföra motsvarande datatekniska åtgärder.

Underrättelseinhämtning som avser datatrafik

Det föreslås att 4 kap. i lagen om militär underrättelseverksamhet innehåller bestämmelser om en ny befogenhet, fastställande av sökbegrepp. Med hjälp av regelbundenheter och särdrag i datatrafiken, vilka anknyter till den aktör som är objekt och vilka fastställts utifrån datatrafikflödet utifrån sökbegrepp är målet att hitta uppgifter som vidare kan användas som sökbegrepp i den egentliga underrättelseinhämtningen som avser datatrafik. Den lagstadgade definitionen av sökbegrepp styr till att sökbegreppen ska avgränsa mängden uppgifter till vad som är nödvändigt.

Förbudet att använda sökbegrepp som avser innehållet i ett meddelande stryks från de egentliga befogenheterna till underrättelseinhämtning som avser datatrafik. I praktiken har det visat sig att uppgifter som ska anses utgöra tekniska data om elektronisk kommunikation inte i alla situationer kan avgränsa informationsmassan på det avsedda sättet, utan att information som kommit till systemet hade kunnat avgränsas till exempel genom att använda ett visst särskilt ord i innehållet. Å andra sidan kan tekniska data om datatrafiken, såsom ett telefonnummer, även finnas i innehållet i ett meddelande.

I fråga om underrättelseinhämtning som avser datatrafik stryks även förbudet att använda en teleterminalutrustning eller en teleadress som finns eller förmodligen finns i Finland. En aktör som är föremål för underrättelse kan komma till Finland under den tid då underrättelseinhämtning som avser datatrafik används, varvid det är nödvändigt att kunna följa aktören fram till dess att bättre riktade metoder för underrättelseinhämtning kan användas.

Avstående från underrättelse om underrättelseinhämtning som avser datatrafik

Underrättelsen om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer slopas. En person som misstänker att han eller hon blivit objekt kan fortfarande framföra en begäran om att underrättelsetillsynsombudsmannen granskar om personen blivit föremål för en metod för underrättelseinhämtning och om man förfarit lagenligt i ärendet.

Inhämtande av information från allmänt tillgängliga källor

Till lagen om försvarsmakten fogas bestämmelser om inhämtande av information från allmänt tillgängliga källor. Informationen kan inhämtas automatiskt och manuellt. Kopplingen till Försvarsmakten kan döljas genom att använda falska, vilseledande eller förtäckta uppgifter. Ett beslut om verksamheten fattas vid den förvaltningsenhet vid Försvarsmakten som genomför underrättelseinhämtningen i enlighet med den interna föreskriften.

Huvudstaben fattar beslut om de förvaltningsenheter som kan använda ovan avsedda täckidentitet och förvaltningsenhetens chef fattar beslut om användning av en täckmantel.

Militärunderrättelsemyndigheterna och stödet för uppgifterna

Det föreslås att Gränsbevakningsväsendet får en befogenhet att biträda militärunderrättelsemyndigheterna i användningen av vissa metoder för militär underrättelseinhämtning. Det föreslås att definitionen av en militärunderrättelsemyndighet utvidgas så att också Armén, Marinen och Flygvapnet till vissa delar ska vara militärunderrättelsemyndigheter. Bland metoderna för underrättelseinhämtning ska de få använda radiosignalspaning och ordinarie användning av informationskällor. Dessutom ska

aktörer som inte är militärunderrättelsemyndigheter i avgränsade situationer ges möjlighet att agera under ledning och övervakning av en militärunderrättelsemyndighet.

Dessutom föreslås att bestämmelser utfärdas om den biträdande rollen för en tjänsteman som avgått från en militärunderrättelsemyndighets tjänst i användningen av metoder för underrättelseinhämtning och om deltagande av personer som genomgått utbildning i användningen av vissa avgränsade metoder för underrättelseinhämtning i en tjänst enligt värnpliktslagen eller i övningar enligt lagen om frivilligt försvar eller i specialuppdrag i sådana.

Övrigt

Teknisk observation av utrustning som hänför sig till en person kan anses vara en ny typ av regleringslösning och varken polislagen eller tvångsmedelslagen innehåller någon motsvarande reglering. Å andra sidan är det redan möjligt att rikta motsvarande tvångsmedel mot en person i fråga om teleavlyssning och teleövervakning.

Det föreslås att man i lagen om militär underrättelseverksamhet gör enskilda ändringar som anknyter till författningsöversynen såväl utifrån preciseringsbehov som observerats i underrättelseverksamheten i praktiken som å andra sidan även ändringar som beror på den övriga lagstiftningen.

Det föreslås att utbytet av information mellan militärunderrättelsemyndigheterna och vissa andra myndigheter utvidgas för utarbetandet av fullgöranderapporter och för situationer där det är nödvändigt att få uppgifter för att utföra ett underrättelseuppdrag. Regleringen kring utbytet av information uppdateras för att motsvara den gällande regleringen för skyddspolisen.

I propositionen föreslås även att man i lagen gör ändringar som ska betraktas som tekniska ändringar, vilka gäller militär underrättelseverksamhet.

I propositionen föreslås även ändringar i lagen om försvarsmakten i fråga om rekryteringens offentlighet vid Försvarsmakten.

4.2 De huvudsakliga konsekvenserna

4.2.1 Ekonomiska konsekvenser

Konsekvenser för den offentliga ekonomin

De föreslagna ändringarna bedöms inte ha betydande ekonomiska konsekvenser. De föreslagna ändringarna kan bedömas effektivisera militärmyndigheternas resursanvändning, då till exempel sökbegrepp som gäller underrättelseinhämtning som avser datatrafik kan fastställas och ändringar i dirigeringen av datatrafiken kan följas ännu bättre och underrättelseinhämtning som avser datatrafik således kan riktas på ett ändamålsenligare sätt.

De föreslagna ändringarna i befogenheterna för de som tjänstgör med stöd av värnpliktslagen och de som deltar i en övning enligt lagen om frivilligt försvar kan öka personalkostnaderna och å andra sidan de kostnader som orsakas av säkerhetsutredningar, men kostnaderna beror i sista hand på i vilken omfattning övningar ordnas och i vilken omfattning tjänstemän som avgått från en militärunderrättelsemyndighets tjänst anställs.

Den nya befogenhet som enligt förslaget föreskrivs för en militärunderrättelsemyndighet för att förhindra användningen av ett datasystem eller störa dess funktion förutsätter att 20 årsverken, det vill säga omkring 2 miljoner euro, allokeras till militärunderrättelsemyndigheten.

De föreslagna nya befogenheterna och de ändringar som gäller riktandet av befogenheterna och de anknutna tillståndstiderna minskar militärunderrättelsemyndighetens arbetsmängd i fråga om domstolsbehandlingen. Detta beror på att inhemsk underrättelseinhämtning som avser datasystem minskar behov av att till en domstol framföra yrkanden som gäller teleavlyssning, teknisk observation av utrustning och teleövervakning. Dessutom minskas antalet yrkanden av teknisk observation av utrustning som hänför sig till en person, eftersom det inte längre finns något behov av att lägga fram ett yrkande om varje anordning som används av en person eller om ett tillstånd. Det är möjligt att antalet yrkanden om behandling av tekniska data sjunker då tillståndstiden ökas till sex månader.

Domstolarnas arbetsmängd som gäller ovan nämnda metoder för underrättelseinhämtning stiger på motsvarande sätt. Militärunderrättelsemyndighetens möjlighet att fatta ett beslut om användning av teleavlyssning i det påskyndande förfarandet sänker domstolarnas arbetsmängd i liten mån, eftersom ett det inte är behövligt att fatta ett beslut vid domstolarnas jour.

Det är möjligt att täcka personalkonsekvenserna ur Försvarmaktens anslag.

De föreslagna ändringarna ger militärunderrättelsemyndigheterna rätt att använda nya metoder för underrättelseinhämtning som hänför sig till datatrafik eller att lagra datatrafik. Detta förutsätter systeminvesteringar. Målet är att täcka investeringarna ur Försvarmaktens anslag.

Propositionen medför ett behov av att utbilda tjänstemännen vid militärunderrättelsemyndigheten och Gränsbevakningsväsendet. Redan för närvarande är utbildning vid Försvarmakten en del av den normala verksamheten och propositionen leder därför inte till nämnvärda ekonomiska konsekvenser.

Gränsbevakningsväsendets möjlighet att bistå en militärunderrättelsemyndighet sänker å sin sida de kostnader som orsakas av militärunderrättelsemyndighetens underrättelseuppdrag, eftersom militärunderrättelsemyndigheten inte behöver ordna sina tjänstemän till ett gränsövergångsställe i brådskande ordning.

Möjligheten för försvarsgrenarna att använda vissa metoder för underrättelseinhämtning förutsätter utbildning, men detta bedöms inte ha ekonomiska konsekvenser.

Propositionen bedöms inte orsaka avsevärda kostnader för Gränsbevakningsväsendet. Gränsbevakningsväsendets bistånd till en militärunderrättelsemyndigheter sker som en del av Gränsbevakningsväsendets normala tjänsteåtgärder. Således kan åtgärderna vidtas med de existerande resurserna.

I fråga om informationsutbytet bedöms förslaget inte ha ekonomiska konsekvenser för myndigheterna. Informationsutbytet sker inom ramen för de nuvarande strukturerna och förutsätter således inte extra resursallokering.

I och med lagförslagen i propositionen kan underrättelsetillsynsombudsmannens uppgifter öka. De nya typerna av befogenheter och slopandet av anmälningsskyldigheten torde förutsätta intensivare övervakning, åtminstone då verksamheten inleds. Det är dock svårt att göra en bedömning på längre sikt av detta vilken omfattar den tid då verksamheten etablerats. Riksdagen

har i varje fall förbundit sig till att tilldela underrättelsetillsynsombudsmannen extra resurser, om det anses vara behövligt för tillräcklig övervakning av underrättelseverksamheten.

Konsekvenser för företagen

Företagen orsakas administrativa kostnader av biståndet till myndigheterna. Det bedöms inte att kostnaderna för kommunikationsförmedlarna stiger från den nivå på vilken de redan nu ligger. De kostnader som uppkommer påverkas även av antalet tillstånd som behövs för att använda vissa metoder för underrättelseinhämtning.

Nya kostnader orsakas för leverantörerna av datacentraltjänster. Kostnader gäller i synnerhet de kopplingar som förutsätts för underrättelseinhämtning som avser datatrafik och som görs i hemlandet. Kostnadsbeloppet beror på hur ofta metoden för underrättelseinhämtning används. Dessutom orsakar tillgången till uppgifter från privata sammanslutningar administrativa kostnader för leverantören av datacentraltjänster på grund av besvarandet av begäranden.

En leverantör av datacentraltjänster har rätt att ur statens medel få en ersättning för direkta investerings- och administreringskostnader som beror på de anordningar och system som krävs av myndigheterna.

4.2.2 Konsekvenser för företagen

Propositionen orsakar administrativa kostnader som bedöms vara små för företagen. De kostnader för myndighetstjänster som orsakas för företagen ökar i liten mån via myndighetsenkäter, förfrågningar eller andra förpliktelser som hänför sig till näringslivets olika branscher.

Cybersäkerhetslagen ställer bland annat en skyldighet för företagen att anmäla avsevärda avvikelser till tillsynsmyndigheten. Lagförslaget ger en militärunderrättelsemyndighet en möjlighet att installera bland annat en programvara i en anordning hos den som är föremål för en metod, använda en privatpersons anordning för att installera en programvara samt göra en koppling som informationsinhämtning som avser datatrafik förutsätter till en del av ett kommunikationsnät som överskrider Finlands gräns utan att den som administrerar det är medveten om detta.

Om ett företag kan uppdaga att en anordning har en främmande programvara som installerats av en militärunderrättelsemyndighet eller att det finns en främmande anordning i kommunikationsnätet, handlar det om en dataskyddsincident. Om incidenten är avsevärd har aktören en skyldighet att underrätta tillsynsmyndigheten om detta.

I regel kan det bedömas att överskridande av tröskeln för en avsevärd incident kan anses vara väldigt exceptionellt. Detta baserar sig på att militärunderrättelseverksamhet redan i princip är hemlig verksamhet som inte ska avslöjas. I varje fall kan detta bedömas att det ger upphov till relativt små kostnader, om ett företag upptäcker en incident. Kostnaderna utgörs av den arbetstid som det tar att göra anmälan eller rapporten om observationen av en enskild avsevärd avvikelse. Till andra delar startar en normal process för hantering av avvikelsen i företaget. Åtgärderna kan orsaka kostnader för företaget. Eventuella skador ersätts således enligt vad som föreskrivs i skadeståndslagen.

I praktiken är det aldrig ändamålsenligt att vidta de föreslagna åtgärderna till exempel genom att utnyttja ett teleföretags kritiska produktionsinfrastruktur. I de föreslagna åtgärderna används

i praktiken en viss enskild anordning, såsom en router, eller en viss del av ett datasystem. I planeringen av åtgärderna ska man därtill noggrant överväga om de orsakar större olägenhet än ringa. I praktiken ska olägenheten alltså synas för en enskild användare som till exempel en tillfälligt långsammare datatrafikförbindelse, inte som en långsammare datatrafikförbindelse för hela kundkretsen i teleföretaget.

Användningen av en anordning som hör till en aktör utanför militärunderrättelsemyndigheten till exempel vid installation eller avinstallation kan orsaka konsekvenser för det företag som tillverkat anordningen med tanke på dess immateriella egendom, avtalskonsekvenser och förtroendet för dess verksamhet. Till denna del bedöms konsekvenserna vara små, eftersom syftet med åtgärderna inte är att till exempel i omfattande grad allmänt installera till exempel kryphål i datatrafikanordningar som tillverkas av ett visst företag redan i tillverkningsskedet. Användning av en enskild anordning för det förslagna syftet kan i praktiken inte orsaka ovan beskrivna skador.

Olägenheten av militärunderrättelsemyndighetens verksamhet för företaget kan i viss mån anses minskas av att en sårbarhet som färdigt finns i ett system eller en anordning, meddelas av underrättelsemyndigheten till de behöriga myndigheterna.

Cybersäkerhetslagens 10 § fastställer även ansvaret för aktörens ledning. Med ledning avses aktörens styrelse, förvaltningsråd eller verkställande direktör samt någon annan som har en jämställbar ställning och som de facto leder dess verksamhet. Det är dock möjligt att det i praktiken är teoretiskt att ledningen anses bära ansvaret på grund av orsaker som beror på militär underrättelseinhämtning, om aktören förfar enligt cybersäkerhetslagen. Åtgärder inom militär underrättelseinhämtning kan för egen del innebära att aktören inte fullgjort sina lagstadgade skyldigheter.

I propositionen föreslås att lagen ändras på så sätt att en militärunderrättelsemyndighet kan genomföra en sådan accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter i en del av ett kommunikationsnät i hemlighet för innehavaren av delen av kommunikationsnätet. I praktiken gäller bestämmelsen för aktörer med ansvar för andra kommunikationsnät än de som är kritiska för Finland, såsom centrala teleföretag. De centrala principerna i lagen om militär underrättelseverksamhet och militärunderrättelsemyndighetens skadeståndsansvar styr till att åtgärder vidtas i smyg i så hög grad som det är möjligt – målet är alltid att hålla verksamheten hemlig. På grund av detta omfattar åtgärder som vidtas i samhällskritisk infrastruktur i praktiken alltid en stor risk för att avslöjas eller orsaka skador, varför accesspunkter till denna del inte genomförs utan medverkan av innehavaren av ett kommunikationsnät.

I propositionen föreslås att lagen ändras på så sätt att utöver kommunikationsförmedlare får även en leverantör av datacentraltjänster skyldigheter att bistå militärunderrättelsemyndigheten. På motsvarande sätt föreslås att den ersättningsskyldighet som föreskrivs i lagen utvidgas till att täcka även leverantörer av datacentraltjänster på samma sätt som kommunikationsförmedlare. Ersättningen är inte lika omfattande som den ersättning som ska betalas till en dataförmedlare enligt lagen om militär underrättelseverksamhet. Eftersom system som gäller metoder för underrättelseinhämtning som hänför sig till telenät används även av andra myndigheter (såsom polisen och Gränsbevakningsväsendet), kan ersättningens omfattning inte behandlas mer ingående i denna proposition. Jämfört med till exempel inhämtande av information som används i brottsbekämpningen, är inhämtandet av information av underrättelsemyndigheterna i telenät mindre omfattande. I varje fall ska ärendehelheten utredas i ett separat projekt, såsom kommunikationsutskottet konstaterat (KoUU 1/2022 rd). Det ovan konstaterade orsakar indirekta små kostnader för leverantörer av datacentraltjänster.

De föreslagna lagändringarna utvidgar en militärunderrättelsemyndighets rätt att få information från privata sammanslutningar. I och med ändringen gäller de skyldigheter som föreslås i bestämmelsen utöver kommunikationsförmedlare även för leverantörer av datacentraltjänster. Utvidgandet kan inte anses vara betydande. Ändringen har inte konsekvenser för bland annat de ända till ända-krypteringar som används i tjänsterna och inga skyldigheter ställs för företaget att öppna sådana eller andra krypteringar eller att installera kryphål.

I propositionen föreslås rätt för en militärunderrättelsemyndighet att få vidta datatekniska åtgärder i ett utländskt datasystem, om det genom datasystemet eller via det kan orsakas ett allvarligt hot mot Finlands försvar eller nationella säkerhet. Genom datatekniska åtgärder är det möjligt att direkt förebygga skador i synnerhet för de aktörer som sköter kritisk infrastruktur. Möjligheten att vidta åtgärder och å andra sidan framgångsrika åtgärder kan anses höja tröskeln för att rikta de allvarligaste cyberhoten mot det finländska samhällets funktion. Påverkan av cyberhot kan på lång sikt bedömas minska kostnaderna för att förbereda sig mot cyberhot och kostnaderna i och med att de skador som orsakas minskar.

Å andra sidan kan förslaget vid en eskalering orsaka en ökad möjlighet att i synnerhet teleföretag blir föremål för cyberattacker. Den risk som åtgärderna orsakar ska bedömas noggrant innan de inleds, men även under den tid då de vidtas. Militärunderrättelsemyndigheten ska med de tillgängliga rimliga metoderna sörja för att i synnerhet de aktörer som ansvarar för Finlands kritiska infrastruktur har tillräcklig information om för att förbereda sig på eventuella följder. Med beaktande av åtgärdernas natur bedöms risken vara liten och exceptionell.

4.2.3 Konsekvenser för samhällsekonomin och näringslivet

Underrättelselagstiftningens konsekvenser för företag, samhällsekonomin och näringslivet ska bedömas som helhet. I bedömningen av lagstiftningens konsekvenser ska man beakta i synnerhet konsekvenserna för digitaliseringsutvecklingen i samhället och företagens verksamhetsförutsättningar, eftersom det med tanke på den ekonomiska tillväxten är nödvändigt för Finland att effektivt utnyttja de möjligheter som informations- och kommunikationsteknologin erbjuder i fråga om ändring av förfaringssätten och förbättring av produktiviteten.

Syftet med lagstiftningen om militär underrättelseverksamhet är att skydda Finland, dess nationella säkerhet och den anknutna samhällsekonomin. Det centrala målet med lagstiftningen om militär underrättelseverksamhet är att inhämta information om hot mot intressen som är centrala för Finlands nationella säkerhet och även samhällsekonomin samt att avvärja dessa. Således kan utvecklingen av underrättelselagstiftningen bedömas höja de utländska staternas tröskel att rikta spionage mot Finland eller annan skadlig verksamhet som bedrivs via datanät eller på annat sätt. Den förbättrade underrättelsekapaciteten minskar dock inte behovet av egna skyddsåtgärder för sammanslutningarna eller individerna och inte heller deras betydelse, utan de förblir fortfarande en av de mest centrala metoderna för att avvärja olika hot. En fungerande reglering och den nya prestandan kompletterar dock säkerheten i Finlands digitala miljö och främjar möjligheterna för näringslivet att skydda sig mot hot som orsakas av utländska stater. I detta hänseende är det av betydelse till exempel att information som fås genom att använda metoderna för underrättelseinhämtning fortfarande kan lämnas till företagen för att avvärja allvarliga hot eller för att försvara viktiga ekonomiska intressen.

Med tanke på samhällsekonomin och verksamhetsförutsättningarna för de företag som verkar som en del av den är det viktigt att författningsgrunden för militär underrättelseinhämtning är tydlig. En tillräckligt exakt och balanserad lagstiftning innebär förutsebarhet i planeringen av företagets verksamhet och investeringsbeslut. I och med att underrättelseregleringens och

dataskyddets betydelse accentueras på den digitala marknaden, kan en exakt, jämbördig och proportionell reglering i bästa fall bedömas vara en positiv konkurrensfaktor för Finland på den internationella marknaden.

Identifiering av hot mot samhället, den kritiska infrastrukturen och bevarande av samhällets ekonomiska livskraft förutsätter ett samarbete mellan den offentliga och privata sektorn. Detta innebär ett smidigt informationsbyte mellan underrättelsemyndigheterna och den privata sektorn. Genom lagförslaget strävar man efter att skaffa en tillräcklig rättsgrund för att militärunderrättelsemyndigheterna ska kunna lämna ut information till företagen för att skydda deras betydande intressen. Information som genererats genom underrättelseinhämtning kan vid behov lämnas till privata företag för att göra det möjligt att avvärja allvarliga hot eller för att förhindra avsevärda ekonomiska förluster. Regleringen kring ärendet omfattar det förslag som är under behandling.

Ett underrättelsesystem som fungerar effektivt och tillförlitligt förutsätter myndighetsinvesteringar i teknologi och kompetens som används i underrättelseverksamhet. De föreslagna befogenheterna att inhämta information förutsätter tekniska investeringar och satsningar på en säker produktutveckling. På grund av verksamhetens natur ska man i investeringarna beakta i synnerhet säkerheten i teknik som upphandlas samt försörjningsberedskapsfrågor som är väsentliga med tanke på systemens funktion. Likaså ska möjligheterna att utnyttja avtalsbaserad serviceproduktion beaktas, eftersom tekniskt kunnande och tekniska resurser oundvikligen måste upphandlas även från den privata sektorn. I en miljö där den digitala tekniken utvecklas snabbt kan detta innebära att nya affärsverksamhetsmodeller, arbetsplatser och kompetenser uppstår i Finland. Myndigheternas teknologinvesteringar kan för vissa högteknologiföretag innebära positiva möjligheter att utveckla de tjänster och den teknik som säkerhetsmyndigheterna behöver.

Näringslivet verkar i en global verksamhetsmiljö som präglas av internationell ekonomi och värdenätverk. I den globala konkurrensen påverkar även små omständigheter staternas konkurrensförmåga. Företagen placerar sin funktioner landspecifikt för att optimera hela sin företagsverksamhet utifrån de egna företagsspecifika konkurrensfördelarna. Etableringsbeslut bygger på helhetsbedömningar med avseende på företagets 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 nogga 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. Den kunskapsintensiva industrins ekonomiska betydelse håller på att öka. Propositionens konsekvenser för företagsverksamheten varierar beroende på bland annat 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. Det väsentliga för IKT-sektorns konkurrenskraft är att regleringen inte förpliktar företagen att försäkra tillförlitligheten i sina produkter eller tjänster till exempel till följd av överlåtelse av krypteringsnycklar, installation

av kryptohål, 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 på finskt 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.

Den gällande lagen om militär underrättelseverksamhet trädde i kraft den 1 juni 2019. Det har inte observerats att lagen direkt påverkat de investeringar som hänför sig till Finland. Finland har fortfarande fått exempelvis till och med stor datacentralinvesteringar under den tid lagen varit i kraft.

För närvarande har myndigheterna en begränsad förmåga att upptäcka statliga spionageprogram eller -operationer som allvarligt hotar den nationella säkerheten. Utvecklingen av den helhet som utgörs av underrättelseinhämtning som avser datatrafik kompletterar avsevärt Finlands skydd mot de allvarligaste datanätshoten. Dessutom kan möjligheten att vidta åtgärder i ett datasystem utanför Finland bedömas förbättra även näringslivets skydd mot de allvarligaste datanätshoten.

En ännu bättre underrättelseinhämtning än tidigare och det förbättrade skyddet samt den höjda tröskeln för att genomföra cyberhot kan på lång sikt bedömas stärka samhällsekonomin, om det inte längre är behövt att använda lika mycket samhällsekonomiska resurser för skyddet mot ett cyberhot och de skador som ett sådant orsakar. I bästa fall förbättrar förslaget Finlands konkurrenskraft som ett säkert land även i fråga om cybermiljön och orsakar kostnadsbesparingar för den offentliga ekonomin.

I propositionen föreslås att ett arvode kan betalas skattefritt till en informationskälla, men även till ett biträde. Utöver vad som föreslås om möjligheten för en aktör utanför myndigheten att exempelvis installera en programvara i en anordning som utgör objekt, ska det även vara möjligt att skattefritt betala ett arvode för sedvanligt bistånd. Utifrån vad som föreskrivits det skattefria arvode som betalas till en informationskälla och det som framgår av dess tillämpningspraxis anses arvoden vara små.

4.2.4 Konsekvenser för informationshanteringen

I informationshanteringslagen föreskrivs bland annat om ordnande och beskrivning av informationshantering, informationslagrens interoperabilitet, genomförande av tekniska gränssnitt och elektroniska förbindelser samt genomförande av informationssäkerhet. Genom informationshanteringslagen säkerställs en enhetlig och kvalitativ hantering samt informationssäker behandling av myndigheternas informationsmaterial så att offentlighetsprincipen förverkligas.

I propositionen föreslås att en ny befogenhet som gäller fastställande av sökbegrepp som gäller underrättelseinhämtning som avser datatrafik fogas till lagen om militär underrättelseverksamhet (67 a § i lagförslag 1). Därtill föreslås även en ändring av regleringen kring behandling av tekniska data om datatrafik (66 § i lagförslag 1) och regleringen kring egentlig underrättelseinhämtning som avser datatrafik (68 och 70 § i lagförslag 1). Ändringar föreslås även i fråga om militärunderrättelsemyndighetens rätt att få uppgifter från andra

myndigheter. Det föreslås att man till lagen om försvarsmakten (8 b § i lagförslag 2) fogar ny reglering som gäller underrättelseinhämtning från allmänt tillgängliga källor. Militärunderrättelsemyndigheten kan med stöd av den föreslagna regleringen på ett mer omfattande sätt än med de nuvarande befogenheterna inhämta och behandla samt lagra uppgifter för att utföra sina uppgifter.

Befogenheten att fastställa sökbegrepp inom den helhet som utgörs av underrättelseinhämtning som avser datatrafik förutsätter att ett nytt datasystem inrättas och en rätt att lagra även data även vid behandling av tekniska data och därtill förutsätter fastställandet av sökbegrepp slutna datamiljöer och behandlingen av data i dessa förutsätter ett domstolstillstånd.

På motsvarande sätt förutsätter rätten att lagra datatrafik för en viss tid och att behandla den ofta att man bygger datasystem med högt dataskydd. De datasystem i vilka information lagrats ska ha gränssnitt till de metoder för underrättelseinhämtning genom vilka informationen behandlas och vilka kräver domstolstillstånd. Det ska vara möjligt att kunna förvissa sig om det domstolstillstånd som är en förutsättning för informationsbehandling.

Dessutom förutsätter inhämtande av information från allmänt tillgängliga källor att ett nytt datasystem grundas. Till andra delar kan de behövliga funktionaliteterna genomföras i de datasystem som redan är i användning.

Det föreslås att samarbetet mellan en militärunderrättelsemyndighet och Gränsbevakningsväsendet görs tätare (18 a § i lagförslag 1, lagförslag 11 och lagförslag 12). Myndigheterna behandlar med tanke på dataskyddskraven motsvarande uppgifter som är känsliga och som ska sekretessbeläggas i sina system redan inom ramen för den nuvarande regleringen. I propositionen föreslås inte ändringar i fördelningen av ansvaret för administreringen och personuppgiftsansvaret för informationssystemen.

I propositionen föreslås inte ändringar i fördelningen av ansvaret för administreringen och personuppgiftsansvaret för informationssystemen. Lagen innehåller exakta och noggrant avgränsade bestämmelser om för vilka ändamål uppgifter får användas och för vems bruk och för vilket ändamål uppgifter kan lämnas ut. Dessutom innehåller lagen exakta och noggrant avgränsade bestämmelser om utplåning av uppgifter. Regleringen bedöms inte orsaka betydande ändringar i sättet att lämna ut uppgifter eller i fullgörandet av kraven enligt informationshanteringslagen och den övriga allmänna lagstiftningen.

Försvarsmakten, en militärunderrättelsemyndighet samt de myndigheter som tar emot uppgifter ska även framöver i behandlingen av data iakttä samma krav som i lagstiftningen redan för närvarande förutsätts för behandling av uppgifter som ska beläggas med sekretess, uppgifter hör till särskilda kategorier av personuppgifter samt känsliga uppgifter. I behandlingen och utlämnandet av uppgifter iakttas utöver de myndighetsspecifika personuppgiftslagarna även kraven i den allmänna dataskyddslagstiftningen, offentlighetslagen och informationshanteringslagen.

Försvarsmakten, en militärunderrättelsemyndighet och andra myndigheter som fungerar som informationshanteringsenheter enligt informationshanteringslagen ska bedöma konsekvenserna av förändringar i informationshanteringen enligt 5 § 3 mom. i informationshanteringslagen och vid behov uppdatera informationshanteringsmodellen, beskrivningen av handlingarnas offentlighet och övrig relevant dokumentation så att de motsvarar den nya regleringens operativa modeller.

Rätten för en militärunderrättelsemyndighet att begära en fullgöranderapport från Enheten för utredning av grå ekonomi förutsätter inte att nya informationssystem byggs. Informationsutbytet sker inom ramen för de nuvarande strukturerna och förutsätter således inte extra åtgärder.

I propositionen föreslås inte ändringar i den gällande regleringen om handlingars offentlighet och sekretess. Parternas rätt att få information har begränsats i den gällande lagstiftningen då det handlar om uppgifter som fås genom metoder för underrättelseinhämtning. Det föreslås att partoffentligheten begränsas på motsvarande grunder även i fråga om uppgifter som fås med de nya föreslagna metoderna för underrättelseinhämtning och ändringarna av dessa.

4.2.5 Övriga konsekvenser för människor och samhällsliga konsekvenser

4.2.5.1 De grundläggande fri- och rättigheterna och de mänskliga rättigheterna

Konsekvenserna av bestämmelserna i lagen om militär underrättelseverksamhet för de grundläggande fri- och rättigheterna har bedömts i mer omfattande grad i den regeringsproposition som ledde till att lagen om militär underrättelseverksamhet stiftades (RP 203/2017 rd). De föreslagna ändringarna är relevanta för flera grundläggande fri- och rättigheter. Dessa är jämlikhet (GL 6 §), rätten till liv, personlig frihet och integritet (GL 7 §), skyddet för privatlivet (GL 10 §), yttrandefriheten och offentligheten (GL 12 §), egendomsskyddet (GL 15 §) och rättsskyddet (GL 21 §). Förhållandet mellan de föreslagna ändringarna till de grundläggande fri- och rättigheter och mänskliga rättigheter som tryggats i grundlagen behandlas i avsnitt 10 om lagstiftningsordningen.

Det uttryckliga omnämnandet av säkerhet i 7 § i grundlagen betonar det allmännas skyldighet till positiv verksamhet för att skydda samhällets medlemmar (RP 309/1993 rd, s. 51). De föreslagna ändringarna har i princip positiva konsekvenser för rätten till liv, personlig frihet och integritet enligt 7 § i grundlagen. Genom tryggheten av en militärunderrättelsemyndighets verksamhet i den föränderliga säkerhets- och teknologimiljön är det möjligt att bättre skydda Finlands försvar, nationella säkerhet och samhällssäkerhet samt de rättsobjekt som hör till deras områden och som ska skyddas. Inga ändringar föreslås i fråga om de hot som är föremål för militär underrättelseinhämtning och som kan anses vara de alla allvarigaste för samhället.

De föreslagna ändringarna, i synnerhet fastställandet av sökbegrepp för underrättelseinhämtning som avser datatrafik, det partiella slopandet av förbudet mot innehållsmässiga sökbegrepp och slopandet av underrättelseskyldigheten är av betydelse med tanke på skyddet för privatlivet.

Fastställandet av sökbegrepp som gäller underrättelseinhämtning som avser datatrafik hänför sig till elektronisk kommunikation i dess maskinspråkform, det vill säga att det inte är möjligt att behandla eller utreda dess innehåll i begriplig form. Genom tekniska metoder är det möjligt att utifrån datatrafiken på maskinspråk bilda nya sökbegrepp, andra än ord på det talade språket, med vilka det är möjligt att bättre än tidigare rikta den egentliga underrättelseinhämtningen som avser datatrafik. Således kan egentlig underrättelseinhämtning som avser datatrafik anses innebära en mindre inskränkning av hemligheten i fråga om förtroliga meddelanden, vilken tryggs i 10 § i grundlagen.

Förslaget om ändring av behandling av tekniska data om datatrafik och fastställandet av sökbegrepp ger militärunderrättelsemyndigheten rätt att lagra uppgifter. Lagringen av uppgifter ingriper i personens integritetsskydd, men detta kan inte bedömas ha avsevärda konsekvenser för en individs grundläggande fri- och rättigheter. Omfattningen av ingreppet kan bedömas vara

avgränsad, eftersom det endast utifrån de lagrade uppgifterna inte är möjligt att dra djupgående slutsatser om en individs personliga liv.

Å andra sidan kan möjligheten enligt förslaget i propositionen att använda sökbegrepp som hänför sig till innehållet i kommunikationen anses förbättra integritetsskyddet. Möjligheten att använda språkliga sökbegrepp tillsammans med ett annat sökbegrepp avgränsar redan i det skede då man använder sökbegrepp som hänför sig till underrättelseinhämtning som avser datatrafik den information som inkommer för fortsatt behandling av militärunderrättelsemyndigheten på ett effektivare sätt än tidigare. Den gällande lagens möjlighet att automatiskt och manuellt behandla datatrafik som motsvarar sökbegreppen överförs således delvis till ett ännu tidigare skede. Detta innebär även att förslaget inte kan anses ha betydande konsekvenser för tillgodoseendet av integritetsskyddet.

Användningen av andra sökbegrepp än sådana som beskriver meddelandets språkliga innehåll kan inte bedömas påverka integritetsskyddet avsevärt. I det aktuella fallet ska sökbegreppet anknyta till ett föremål enligt 4 § i lagen om militär underrättelseverksamhet i enlighet med domstolstillståndet. Detta kan anses förbättra effektiviteten i militärunderrättelsemyndighetens underrättelseinhämtning med tanke landets försvar och skyddet av den nationella säkerheten samt att bekämpningen av de anknutna hoten förbättrar säkerheten för personer i Finland. I situationer där det detta sökbegrepp finns inom en så kallad inkapslad datatrafik, kan inhämtandet av information inte anses utgöra nya konsekvenser för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna.

Fastställandet av sökbegrepp och slopandet av förbudet mot innehållsmässiga sökbegrepp kan för egen del bedömas förbättra integritetsskyddet i och med att underrättelseinhämtning som avser datatrafik riktas på noggrannare sätt. På samma gång effektiviseras naturligtvis underrättelseinhämtningen och dess resultat förbättras.

Enligt lagförslaget kan en militärunderrättelsemyndighet använda även utomståendes anordningar eller datasystem, om det är nödvändigt för att installera eller avinstallera en metod eller en programvara. En enskild åtgärd bedöms inte ingripa avsevärt i egendomsskyddet, eftersom längden på en åtgärd kan anses vara relativt kort. I varje fall utfärdas uttryckliga bestämmelser om att åtgärden ska avgränsas till en ringa olägenhet och å andra sidan ska myndigheten betala skadestånd enligt skadeståndslagen för en större skada.

I fråga om de metoder för underrättelseinhämtning som innebär det mest avsevärda ingreppet i de grundläggande fri- och rättigheterna och de mänskliga rättigheterna föreslås att beslutsfattandet fortfarande äger rum i en domstol. Begränsningen av de grundläggande fri- och rättigheterna och de mänskliga rättigheterna till följd av användningen av metoderna för underrättelseinhämtning övervakas fortfarande med flera olika metoder. Genom effektiv och flerskiktig övervakning i förväg, realtid och i efterskott förebyggs missbruk som äventyrar de grundläggande fri- och rättigheterna och de mänskliga rättigheterna och uppkomst av dålig praxis.

I propositionen föreslås att regleringen kring underrättelse om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer i lagen om militär underrättelseverksamhet ändras på så sätt att användningen av en metod för underrättelseinhämtning inte underrättas till den som blivit objekt för användning av den. I en bred kontext kan detta för egen del anses förbättra tillgodoseendet av de grundläggande fri- och rättigheterna, eftersom militärunderrättelsemyndigheten inte behöver börja utreda uppgifter om alla som blivit föremål för användningen av en metod för underrättelseinhämtning som omfattas av anmälningsskyldigheten. Detta kan i sista hand innebära användning av metoder för

underrättelseinhämtning och inhämtande av information för att utreda till vem meddelandet ska göras rent konkret. Regleringen kring underrättelseskyldigheten har i samband med att lagen stiftades motiverats med rättsskyddsaspekter.

De föreslagna ändringarna har således en kontaktyta med tillgodoseendet av rättsskyddet. Den föreslagna ändringen bedöms inte försämra rätten till rättsskydd. I propositionen föreslås inte ändringar i rätten att få hänskjuta ett ärende för att utredas av underrättelsetillsynsombudsmannen eller till det domstolsförfarande som användningen av en metod för underrättelseinhämtning förutsätter. Underrättelsetillsynsombudsmannens uppgift är att övervaka underrättelseverksamhet och dess lagenlighet på ett övergripande sätt i förväg, i realtid och i efterskott, varvid det i övervakningen är möjligt att rikta uppmärksamhet på verksamheten även ur enskilda personers synvinkel. Underrättelsetillsynsombudsmannen har även till uppgift att uttryckligen övervaka att rättsskyddet tillgodoses. Det ovan konstaterade avser att ansvaret för att tillgodose rättsskyddet övergår tydligare till underrättelsetillsynsombudsmannen.

Underlåtenhet att ge meddelandet kan inte anses avsevärt förändra personens ställning i fråga om användningen av rättsmedel. I första hand ansvarar myndigheten själv för att underrättelsemyndigheten agerar lagenligt och att metoderna för underrättelseinhämtning riktas rätt. Underrättelsetillsynsombudsmannen, som har till uppgift att aktivt ingripa i lagstridig förfarande, innebär en extern garanti för rättsskyddet i verksamhet. Den föreslagna ändringen överför tydligare ansvaret för att rättsskyddet tillgodoses till underrättelsetillsynsombudsmannen, som redan för närvarande i regeln ansvarar för detta.

Således kan underrättelsetillsynsombudsmannen anses sörja för rättsskyddet för den som blivit föremål användningen av en metod för underrättelseinhämtning, även om den som blivit föremål inte får något meddelande eller information om detta. Om underrättelsetillsynsombudsmannen hänskjuter ärendet till förundersökningen, får dock personen informationen om att han eller hon blivit föremål för en metod via straffprocessen. Utöver vad som konstaterats ovan förutsätter underrättelseinhämtning som avser datatrafik ett domstolstillstånd.

Den föreslagna nya befogenheten, underrättelseinhämtning i Finland som avser statliga aktörers datasystem, kan innebära en inskränkning av skyddet för privatlivet för en annan än statlig aktör, om man behandlar också andra uppgifter än uppgifter om den statliga aktören i det datasystem som är föremål för användningen av befogenheten. Dessa situationer omfattas dock av direktutplåningsregleringen och regleringen kring avbrytande av användningen av metoden för underrättelseinhämtning, via vilka den information som når behandling senast avgränsas till endast vad som är nödvändigt.

De föreslagna ändringarna har i viss mån konsekvenser för tillgodoseendet av den grundlagstryggade offentlighetsprincipen. Regleringen föranleds emellertid av ett vägande samhälleligt intresse som förutsätter att det görs ett avgränsat undantag från offentlighetsprincipen.

De föreslagna ändringarna som gäller tryggheten av en informationskälla kan anses ha positiva konsekvenser för skyddet av de grundläggande fri- och rättigheterna och de mänskliga rättigheterna för en informationskälla.

De föreslagna ändringarna som gäller regleringen om ledigförklaring av en tjänst i 36 a § i lagen om försvarsmakten har en kontaktpunkt med det rättsskydd som tryggas i 21 § i grundlagen. I och med den föreslagna ändringen har andra än dem som ansöker en tjänst enligt 2 mom. i

paragrafen inte nödvändigtvis rätt att få information om identiteten på den person som valts till tjänsten eller på dem som sökt tjänsten. I vissa situationer kan detta ha en konsekvens för sökandenas möjligheter att bedöma om en tjänst tillsatts på behörigt sätt. Personerna har dock fortfarande möjlighet att framföra klagomål om en myndighets förfarande då den tillsatt en tjänst. Huvudregeln är fortfarande att tjänster tillsatts offentligt och undantaget hänför sig till en relativt liten grupp personer med specialkunnande, varför konsekvenserna kan anses hänföra sig till en avgränsad grupp personer.

De föreslagna ändringarna som gäller regleringen om ledigförklaring av en tjänst i 36 a § i lagen om försvarsmakten har en kontaktpunkt med den jämlikhet som tryggas i 6 § i grundlagen. Generellt sett är det utifrån en persons namn fram till en viss punkt möjligt att göra en bedömning av personens kön och då namnuppgifterna inte fås av dem som sökt en tjänst, har sökandena inte möjlighet att fullt ut bedöma om jämlikheten har tillgodosetts i rekryteringen. I enlighet med den gällande lagen har sökandena dock möjlighet att framföra klagomål i ärendet till justitiekanslern i statsrådet eller riksdagens justitieombudsman och väcka talan utifrån arbetsdiskriminering enligt lagen om jämställdhet mellan kvinnor och män (609/1986), diskrimineringslagen (1325/2014) eller 47 kap. 3 § i strafflagen (39/1998).

I propositionen har inksräkningarna av de grundläggande fri- och rättigheterna och de mänskliga rättigheterna genom regleringen avgränsats till vad som är nödvändigt för att skydda intressen som är viktiga för samhället, i synnerhet i anknytning till den nationella säkerheten och försvaret av landet. Tillämpningsområdet för de bestämmelser som föreslås i propositionen hänför sig till personer, specificerade grupper och aktörer, som kan anses kunna vara föremål för inhämtande av information och åtgärder som är effektiv och förenlig med proportionalitetsprincipen och således bäst främjar samhällets och individernas säkerhet.

Förslaget bedöms stärka tillgodoseendet av de nämnda grundläggande fri- och rättigheterna i samhället i den mån att de konsekvenser för de grundläggande fri- och rättigheterna vilka följer av ändringarna av befogenheterna för inhämtande av information och databehandlingen är motiverade och proportionella. Dessutom ska det beaktas att de bättre förutsättningarna än tidigare att rikta metoderna för underrättelseinhämtning minskar behandlingen av uppgifter som gäller utomstående och som är onödiga för föremålet för militär underrättelseinhämtning.

4.2.5.2 Jämlikhet och jämställdhet mellan könen

I 9 § i lagen om militär underrättelseverksamhet finns det bestämmelser om förbudet mot diskriminerande underrättelseinhämtning och de föreslagna ändringarna av underrättelseinhämtning som avser datatrafik och behandlingen av tekniska data bedöms inte ha konsekvenser för jämlikheten och jämställdheten mellan könen.

Den föreslagna ändringen av 91 § i lagen om militär underrättelseverksamhet möjliggör att dem som är i en övning enligt 18 och 19 § i lagen om frivilligt försvar deltar i användningen av vissa metoder för underrättelseinhämtning under uppsikt och övervakning av en tjänsteman. Kvinnor och män som uppfyller förutsättningarna men som inte avlagt beväringstjänsten eller som inte längre hör till reserven kan delta i specialuppdrag under frivilliga övningar. Ändringsförslaget bedöms öka jämlikheten, då även personer som deltar i ovan beskrivna övningar kan delta i militär underrättelseinhämtning. Sannolikt innehåller dock en väldigt begränsad personkrets specialkunnande inom militär underrättelseinhämtning, varför konsekvensen inte har något värst stor omfattning.

4.2.5.3 Myndigheternas verksamhet

Försvarsmakten

De hot som kan identifieras genom militär underrättelseinhämtning är internationella och allvarliga hot och de hänför sig till statens centrala säkerhetsintressen. I och med den nu behandlade propositionen kan en militärunderrättelsemyndighet på ett ännu bättre och effektivare sätt till stöd för beslutsfattandet ta fram information som är betydelsefull för Finlands säkerhet med avseende på utländska aktörer och förhållanden. I och med propositionen bedöms statsledningen och Försvarsmaktens ledning få bättre förmåga att reagera på hot som medför fara för Finland. Den utökade informationen förbättrar militärunderrättelsemyndighetens förmåga att informera den högsta statsledningen om förändringar i Finlands säkerhetsmiljö.

Den föreslagna regleringen gör att militärunderrättelsemyndigheten och Skyddspolisens samarbete blir tätare och även att samarbetet med Gränsbevakningsväsendet blir tätare. Det ännu mer omfattande samarbetet med Gränsbevakningsväsendet förutsätter att jourarrangemangen ombesörjs.

Behandlingen av tekniska data om datatrafik orsakar i vissa mån extra kostnader för militärunderrättelsemyndigheten.

Propositionen ställer höga kvalitetsmässiga, utbildningsmässiga och rättsliga krav på genomförandet.

Den föreslagna regleringen förbättrar Försvarsmaktens förmåga att sköta dess lagstadgade uppgifter.

Vissa förslag bedöms spara på de behöriga myndigheternas resurser. Eftersom det till följd av förslaget inte framöver längre finns något behov av att ansöka om och handlägga ett nytt tillstånd varje gång samma misstänkta börjar använda en ny teleadress eller teleterminal som är förenlig med tillståndet och väsentlig med tanke på inhämtandet av information, kommer antalet domstolsförhandlingar om teletvångsmedel sannolikt att minska och därmed görs besparingar i fråga om de resurser som behövs för dessa.

Slopandet av anmälningsskyldigheten för annan underrättelseinhämtning än underrättelseinhämtning som avser datatrafik hos statliga aktörer har en inverkan som minskar den administrativa bördan. Underrättelseskyldigheten enligt den gällande lagen kräver resurser såväl hos militärunderrättelsemyndigheten som hos den domstol som behandlar ärenden som gäller uppskov eller avstående från underrättelse i enlighet med 89 § 6 och 7 mom. i lagen om militär underrättelseverksamhet.

Det föreslagna inhämtandet av information från allmänt tillgängliga källor, skyddet för sådant inhämtande av information och det anknutna beslutsfattandet förutsätter utbildning och att processer skapas i anknytning till beslutsfattandet. Försvarsmakten har redan etablerade förfaringssätt i underrättelseinhämtningen, varför detta inte bedöms orsaka någon avsevärd konsekvens för de behövliga resurserna och inte heller kräver nya datasystem.

I enlighet med propositionen kommer användningssituationerna eventuellt att öka vad gäller metoder för underrättelseinhämtning som genomförs under uppsikt och övervakning av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman. Detta

bedöms öka utbildningsbehoven, vilket dock kan möjliggöras som en del av den normala verksamheten.

Skyddet av identiteten på dem som ansöker om en tjänst från och med ansökningsprocessen förbättrar möjligheten till ändamålsenlig användning av personalresursen och förbättrar militärunderrättelsemyndighetens möjlighet att som arbetsgivare ännu bättre beakta de arbetsgivarskyldigheter som gäller arbetssäkerheten. Ett viktigt element avseende sekretessen för personalens identifieringsuppgifter är den förbättrade arbetssäkerheten för en individ och skyddet av dennes närkrets.

Gränsbevakningsväsendet

Det föreslås att en ny uppgift, deltagande i militär underrättelseinhämtning, föreskrivs för Gränsbevakningsväsendet. För Gränsbevakningsväsendet föreskrivs en möjlighet att stödja militärunderrättelsemyndigheterna genom att vidta enskilda åtgärder som hänför sig till vissa metoder för underrättelseinhämtning på begäran av militärunderrättelsemyndigheten.

De nya befogenheterna till underrättelseinhämtning förutsätter fortbildning av Gränsbevakningsväsendets personal. Största delen av befogenheterna till underrättelseinhämtning är i sig inte nya metoder för Gränsbevakningsväsendet, utan de används endast i ett nytt syfte. Gränsbevakningsväsendets deltagande i underrättelseinhämtningen bedöms inte heller till andra delar orsaka avsevärda ekonomiska konsekvenser.

Den nya uppgift som föreskrivs för Gränsbevakningsväsendet bedöms i liten mån påverka personalens arbetsmängd, eftersom åtgärder vidtas i samband med Gränsbevakningsväsendets övriga lagstadgade uppgifter. Gränsbevakningsväsendet kan dock vägra att tillmötesgå en begäran av en militärunderrättelsemyndighet, om det inte har någon faktisk möjlighet att stödja denna myndighet till exempel på grund av brist på resurser eller prestationsförmåga eller brådskan för en egen lagstadgad uppgift för Gränsbevakningsväsendet.

Den nya uppgift som föreskrivs för Gränsbevakningsväsendet, deltagande i militär underrättelseinhämtning, och de befogenheter som används vid militär underrättelseinhämtning förbättrar Gränsbevakningsväsendets och Försvarsmaktens samarbete samt främjar även den militära underrättelseinhämtningen.

Underrättelsetillsynsombudsmannen

Underrättelsetillsynsombudsmannens årsberättelse avseende år 2025 redogör för att elva begäranden om undersökning framförts till underrättelsetillsynsombudsmannen åren 2023 och 2024 och att ett klagomål tagits upp för prövning under bägge åren. Från och med underrättelsetlagarnas ikraftträdande har antalet begäranden om undersökningar per år varierat mellan 20 och 7.

Det föreslagna slopandet av anmälningsskyldigheten kan öka antalet begäranden om undersökning, om man upplever att slopandet av anmälningsskyldigheten försämrar deras rättsskydd och man aktivare än tidigare börjar utöva sin primära garanti för rättsskydd.

Å andra sidan kan det bedömas att människornas vilja att göra begäranden om undersökning och klagomål förblir oförändrad. Detta undanröjer dock inte möjligheten att till exempel antalet begäranden om undersökning och klagomål på grund av fall som är i offentligheten ökar

tillfälligt till och med avsevärt. I varje fall är det sannolikt att aktivare information än tidigare ska ges om möjligheten att framföra en begäran om undersökning eller ett klagomål till underrättelsetillsynsombudsmannen.

I och med den föreslagna ändringen av 20 § i lagen om militär underrättelseverksamhet har en utländsk behörig tjänsteman i avgränsade situationer rätt att på finskt territorium delta i användningen av en metod för underrättelseinhämtning utifrån ett beslut av huvudstabens underrättelsechef. Militärunderrättelsemyndigheten ansvarar alltid för att användningen av en metod för underrättelseinhämtning är lagenlig. Det är möjligt att volymen på den verksamhet som underrättelsetillsynsombudsmannen övervakar växer i liten mån i och med att det internationella samarbetet ökar.

I och med de föreslagna ändringarna avseende underrättelseinhämtning som avser datatrafik och de nya befogenheterna att inhämta information kan det förväntas att underrättelsetillsynsombudsmannens övervakningsbesök ökar en aning. År 2023 uppgick antalet övervakningsbesök till 171 och år 2024 till 153. Även framöver ska tillräckliga resurser säkerställas för underrättelsetillsynsombudsmannen.

Möjligheten för Armén, Marinen och Flygvapnet att använda radiosignalspaning och underrättelseinhämtning i dess grundform ökar i ringa mån underrättelsetillsynsombudsmannens tillsynsåtgärder.

Konsekvenser för övriga myndigheter

Genom 37 a § i lagförslag 10 ges militärunderrättelsemyndigheten rätt att uppdatera sitt eget informationssystem genom att jämföra de uppgifter som ingår i det med andra myndigheters personregister. Den föreslagna bestämmelsen har konsekvenser för de myndigheter från vars system militärunderrättelsemyndigheten uppdaterar personuppgifterna i det egna informationssystemet. Militärunderrättelsemyndigheten har rätt att få uppgifterna avgiftsfritt. Extraheringen av uppgifter från datasystem för att granskas och det anknutna eventuella arbetet med att slå samman uppgifter kan orsaka kostnader och extra arbete för den personuppgiftsansvarige. Man strävar dock efter att beakta detta i begäranden om information som gäller material och i avgränsningen av dessa. I praktiken orsakar en begäran om information i viss mån en administrativ börda för mottagaren av begäran.

Bedömning av de utrikes- och säkerhetspolitiska konsekvenserna

Den nya befogenheten att störa funktionen i ett datasystem utanför Finlands gränser förutsätter nya typer av processer för beslutsfattande. De åtgärder som vidtagits med stöd av bestämmelsen kan beroende på dess natur ha till och med avsevärda utrikes- och säkerhetspolitiska konsekvenser.

Redan för närvarande innehåller 15 § i lagen bestämmelser om samordnande av underrättelseverksamheten, där man förberedelsevis behandlar även underrättelseverksamhet, om den kan bedömas ha utrikes- och säkerhetspolitiska konsekvenser. Påverkan av funktion i ett datasystem utanför Finlands gräns förutsätter utveckling av uppgifterna för sammansättningen enligt 15 § på ett sätt som motsvarar kraven på den nya typen av verksamhet.

Utrikes- och säkerhetspolitiskt betydelsefulla åtgärder behandlas förberedelsevis i det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president.

4.2.5.4 Den nationella säkerheten och landets försvar

Bättre uppföljning av tekniska och datatekniska förändringar tryggar att militärunderrättelsemyndigheten har förmåga att ta fram uppdaterad information till stöd för beslutsfattandet. Dessutom har säkerställandet av ett sömlöst internationellt samarbete en positiv inverkan på såväl den nationella säkerheten som Finlands verksamhet som en del av alliansen och samarbetet med likasinnade stater.

Antalet kommunikationsnät och datasystem och deras betydelse som en del av produktionen av de tjänster som krävs för samhällsfunktionen och samhällets kritiska infrastruktur ökar kontinuerligt. Cyberhoten och -attackerna har ökat och cyberattackerna utvecklats ständigt i takt med att tekniken utvecklas. De funktioner som är kritiska för samhället är allt mer beroende av datasystem och kommunikationsnät och cyberstörningar i dessa kan ha betydande skadliga konsekvenser för föremålet för störningen, men även för samhället i större omfattning. Även förändringarna i utrikes- och säkerhetspolitiken har återverkningar på cybermiljön. Överbelastningsattacker, intrång, sabotageprogram och riskerna i den statliga verksamheten har ökat och hotnivån har stigit. Cyberattacker används som en del av hybridpåverkan av samhället. Möjligheten att vidta åtgärder i ett datasystem som finns utomlands vilka avbryter eller stör skadliga cyberverksamhet förbättrar den nationella säkerheten och förutsättningarna att försvara landet. I bästa fall leder åtgärderna till att de aktörer som ansvarar för cybersäkerheten inte behöver använda samma mängd resurser som i nuläget för att förhindra skadliga cyberverksamhet.

Genom propositionen stärks för egen del samhällets allmänna cybersäkerhetsnivå. Genom propositionen förbättra verksamhetsförutsättningarna för de myndigheter som är centrala med tanke på samhällets funktion i den förändrade verksamhetsmiljön. Målet med propositionen är att för egen del undvika avbrott som orsakas av cyberstörningar i kontinuiteten för tjänster eller funktioner som är centrala för samhällets funktion, eftersom en störning i utbudet av en kritisk tjänst kan orsaka en avsevärd skada för samhället. En störning i en funktion som är kritisk för samhället (till exempel i energiproduktionen eller kommunikationsnätets funktion) kan avsevärt påverka även utbudet av andra kritiska tjänster samt orsaka vittgående skadliga konsekvenser i samhället. Dessutom kan konsekvenser för kontinuiteten i vissa kritiska tjänster förutom ekonomiska förluster även orsaka till exempel hot mot medborgarnas liv och hälsa.

Propositionen innehåller även förslag som stärker samarbetet och informationsutbytet mellan myndigheterna och andra aktörer. Detta kan bedömas bidra till att förbättra förmågan att tåla cyberstörningar för de verksamhetsområde och tjänster som är centrala för samhället och dess funktion.

Kommunikationsnäten och datasystemen är globalt kopplade till varandra och också en cyberattack eller -störning som riktar sig mot en annan stat kan ha följdverkningar för Finland.

Propositionen bedöms ha även indirekta konsekvenser för medborgarnas säkerhet genom att en störningsfri funktion i samhället främjas. Målet med propositionen är att minska antalet cyberhot och deras konsekvenser för infrastruktur som är kritisk för samhällets funktion. Utredning av synliga cyberstörningar och underlåtenhet att ingripa i dessa kan påverka medborgarnas upplevelse av säkerheten i samhället.

Samarbetet med Gränsbevakningsväsendet kan bedömas förbättra landets försvar och skyddet av den nationella säkerheten, då inhämtandet av information kan inledas effektivare än tidigare direkt då ett objekt identifierats och anlänt till gränsområdet.

Användningen av reservister och deltagare i en frivillig övning i vissa militära underrättelseuppdrag ökar möjligheterna för värnpliktiga och frivilliga att delta i Försvarmaktens verksamhet. Försvarmakten kan utnyttja de värnpliktigas specialkunnande i högre grad än tidigare och detta kan anses bidra till att förbättra viljan att försvara landet. Försvarmakten kan utveckla värnplikten i en riktning, där en ännu större grupp värnpliktiga kan erbjudas utbildning som drar nytta och utvecklar deras specialkunnande ännu bättre.

4.2.5.5 Informationssamhället och dataskyddet

De ändringar som gäller myndigheternas informationsutbyte bedöms ha positiva konsekvenser för informationssamhället och dataskyddet. I synnerhet utlämnande av uppgifter om skadliga datorprogram och skadliga kommandon ger informationsmottagaren bättre förutsättningar att skydda sig mot dessa hot. Detta kan för egen del anses underlätta myndigheternas och de övriga aktörernas samarbete för att skydda sig mot dessa hot och minska konsekvenserna av dessa.

Möjligheten att ingripa i funktionen i ett skadligt datasystem utanför Finlands gräns förbättrar säkerheten i det finländska informationssamhället. Möjligheten att agera kan bedömas höja tröskeln för att vidta skadliga åtgärder då hotaktörerna upptäcker att deras verksamhet störs. Dessutom ger den nya befogenheten en möjlighet att avbryta sådan skadlig verksamhet i ett tidigare skede än för närvarande. Möjligheten för en militärunderrättelsemyndighet att ingripa i verksamheten i ett utländskt datasystem kan anses förbättra informationssamhällets resiliens. Till denna del kan konsekvenserna vara till och med avsevärda i vissa situationer.

De föreslagna ändringarna påverkar inte företagens möjligheter att erbjuda till exempel ända till ända-kryptering (E2EE). I lagförslagen föreslås inte att man underlättar eller möjliggör att militärunderrättelsemyndigheterna enklare får allmän tillgång till företagens system eller tjänster. Lagförslagen bedöms inte äventyra de kommersiella aktörernas direkta förtroendekapital, rätten till privat kommunikation samt bevarandet av företagsförmögenhetens värde samt ombesörjandet av de ekonomiska förutsättningarna för näringsverksamhet. Ända till ända-kryptering kan fortsättningsvis bedömas vara nödvändig för Finlands övergripande säkerhet.

Den föreslagna rätten att använda en anordning eller del av ett kommunikationsnät som hör till en instans utanför militärunderrättelsemyndigheten kan i enskilda fall bromsa eller skada denna instans datatrafikförbindelse eller systemfunktion. Konsekvenserna bedöms dock vara små. Det är dock möjligt att militärunderrättelsemyndigheten då den planerar åtgärder inte kan förbereda sig på alla överraskande situationer och att åtgärden leder till en olägenhet som är större än ringa. Eventuella skador ska ersättas enligt skadeståndslagen.

Syftet med de myndighetsåtgärder som vidtas med stöd av förslaget är dock att utveckla landets försvar, beredskapen och den nationella säkerheten och därmed även främja rättsobjekt som anknyter till dataskyddet i datasystemen och kommunikationsnäten. De föreslagna bestämmelserna har utarbetats med beaktande av konstitutionella synvinklar som gäller skyddet för privatlivet och man har strävat efter att begränsa dessa till endast vad som är nödvändigt i genomförandet av syftet med propositionen. Den positiva konsekvensen för dessa rättsobjekt kan bedömas vara till och med avsevärda.

Propositionen bedöms inte ha konsekvenser för det dataskydd som myndigheterna ansvarar för, utan dataskyddet tillgodoses i enlighet med den gällande lagstiftningen.

4.2.5.6 Gränsöverskridande konsekvenser

De föreslagna ändringarna om påverkan av funktionen i ett datasystem utanför Finlands gränser kan ha konsekvenser för Finlands internationella relationer. Enligt propositionen har en militärunderrättelsemyndighet rätt att förhindra användningen av ett datasystem utanför Finland och sabotera eller ändra dess funktion. Internationellt sett handlar det om ett jämförelsevis vanligt förfaringssätt inom underrättelseverksamhet och sådan verksamhet har i princip inte haft betydliga konsekvenser för de mellanstatliga relationerna. Det är möjligt att justera intensiteten på de åtgärder som föreslagits i propositionen på det sätt som situationen förutsätter och således kan även eskaleringsrisken justeras tämligen noggrant. För närvarande ger en tämligen liten åtgärd en avsevärd nytta för Finlands nationella säkerhet.

Vidtagandet av åtgärder förutsätter ett intensivt samarbete med den stat som är föremål för åtgärden i en situation där staten vänligt inställd. I första hand ska en ovan avsedd stat kunna vidta de behövliga åtgärderna för att främja och undanröja hotet. Detta är dock inte möjligt i alla situationer.

De åtgärder som vidtas ska vara lämpliga och proportionella i varje situation. Det kan dock inte uteslutas att staterna i syfte att driva egna intressen lägger fram sådan verksamhet som en mellanstatlig fejd, vilket Finlands statsledning ska bereda sig på och eventuellt även ska ta ställning till. Åtgärderna kan dock i vissa fall leda till en eskalering, om den stat som är föremål för åtgärderna så vill. I princip strävar man dock alltid efter att hålla den som utför åtgärden hemlig.

Förslaget kan å andra sidan förväntas ha en positiv konsekvens för Finlands anseende bland likasinnade stater.

Möjligheten att vidta åtgärder som riktas på ett datasystem utanför Finlands gräns kan förbättra Finlands ställning på det internationella planet visavi vänligt inställda stater och således ge en möjlighet till ett ännu djupare samarbete. I och med de vidtagna åtgärderna kan de dessutom bedömas höja tröskeln för att rikta skadliga cyberåtgärder mot Finland.

Fastställandet av nya sökbegrepp kan för egen del anses förbättra Finlands ställning i det internationella samarbetet. Utifrån Finlands geografiska ställning och kunnande kan det bedömas att Finland har goda förutsättningar att fastställa sökbegrepp och genom de uppgifter som inhämtats på detta sätt få en bättre ställning på internationella forum.

Hjälp för att en informationskälla ska överskrida gränsen kan även ha konsekvenser för Finlands internationella relationer, i synnerhet om informationskällan haft en hög ställning i samhället i avgångslandet.

5 Alternativa handlingsvägar

5.1 Handlingsalternativen och deras konsekvenser

Bibehållande av nuläget anses inte vara ett ändamålsenligt alternativ redan på grund av att riksdagen i samband med att lagen om militär underrättelseverksamhet stiftades (FvUB 35/2022 rd) har förutsatt att regeringen ser till att lagstiftningen är uppdaterad i en föränderlig verksamhetsmiljö och säkerställer tillräckliga resurser för underrättelseverksamheten och övervakningen av den. I den rådande världspolitiska situationen utvecklas tekniken och datatrafikförbindelserna i en allt mer tilltagande takt, vilket även förutsätter att militärunderrättelsemyndigheternas förfaringssätt utvecklas. Fram till en viss punkt kan en

militärunderrättelsemyndighet rikta sin verksamhet i en föränderlig verksamhetsmiljö även med de gällande befogenheterna, men i den praktiska underrättelseverksamheten har man observerat även sådana ändringsbehov som förutsätter att underrättelselagstiftningen uppdateras.

Helheten av underrättelseinhämtning som avser datatrafik förutsätter att en militärunderrättelsemyndighet har information om de anordningar och den kommunikationsteknik som används i globala kommunikationsnät. I propositionen föreslås att en militärunderrättelsemyndighet vid behandlingen av tekniska data kan behandla tekniska data för att fastställa en del av ett kommunikationsnät och därtill för att följa dirigeringen av och ändringar i datatrafiken. Om den avsedda analysen inte kan göras, kan en militärunderrättelsemyndighet i praktiken inte få information till exempel om den datatrafikteknik som används i en stat som militärt sett är betydande för Finland. Information om de datatrafikanordningar som används är synnerligen betydelsefull för att kunna rikta underrättelseinhämtning som avser datatrafik på ett ändamålsenligt sätt och å andra sidan för att datatrafiken ska kunna packas upp till en tolkbar form.

I praktiken är det omöjligt att få information från den aktör som administrerar ett kommunikationsnät i en främmande stat. I vissa situationer kan det dock vara möjligt att inhämta information med andra metoder, men det kräver onödigt mycket resurser och orsakar en avsevärd fara för livet och hälsan för den tjänsteman som inhämtar informationen.

Å andra sidan kan sammanslutningarnas skyldigheter utvidgas till att på ett omfattande sätt gälla tekniska data om ett kommunikationsnät, men detta orsakar kostnader för företagen. Inte heller ur EU-rättens synvinkel kan omfattande skyldigheter att lämna ut information anses vara förenliga med syftet. På grund av naturen på militär underrättelseinhämtning är det inte heller önskvärt att i för hög grad förlita sig på externa aktörer.

Fastställande av sökbegrepp föreslås som en ny befogenhet i den helhet som omfattar underrättelseinhämtning som avser datatrafik. Med beaktande av den tilltagande takten i den tekniska utvecklingen är det betydelsefullt att kunna fastställa sökbegrepp. Utan ändamålsenliga sökbegrepp, riktar sig underrättelseinhämtning som avser datatrafik inte på ändamålsenligt sätt.

I den tekniska utvecklingen, som i det rådande världspolitiska läget är militärt driven, kan till exempel kommunikationsteknikerna förändras snabbt och de införs i omfattande grad i en ännu snabbare takt än tidigare. Om ett objekt för underrättelseinhämtning inte längre använder en tidigare kommunikationsteknik, utan på en gång byter den till en helt ny teknik, riktas de tillgängliga sökbegreppen inte längre mot datatrafiken hos den aktör som är föremål för underrättelseinhämtningen. I så fall är den finländska underrättelsemyndigheten i praktiken helt beroende av det internationella samarbetet. Med beaktande av Finlands geografiska ställning och kunnande, kan fastställandet av nya sökbegrepp ha en betydelse som till och med kan vara stor.

Vid behandling av tekniska data och fastställandet av sökbegrepp är det även centralt att jämföra data med historikdata. På så sätt är det möjligt att säkerställa uppgifterna till en viss punkt innan till exempel ett nytt sökbegrepp används i den egentliga underrättelseinhämtningen som avser datatrafik. Om detta inte kan göras, kan det leda till att underrättelseinhämtning som avser datatrafik används med inexakta sökbegrepp och att onödig information inhämtas.

Ett alternativ är att tillåta underrättelseinhämtning som avser datatrafik i massform, där man slopar de olika partiella befogenheterna i den helhet som utgörs av underrättelseinhämtning som avser datatrafik. Detta är dock inte möjligt enligt Finlands grundlag.

Om de föreslagna ändringarna inte görs, leder det till en försämrad förmåga för militärunderrättelsemyndigheterna att agera i den rådande säkerhetsmiljön, där andra aktörer konstant utvecklar sina egna förmågor. Detta kan bidra till att äventyra syftet med militär underrättelseinhämtning, det vill säga att producera information till stöd för den högsta statsledningens beslutsfattande för att utföra Försvarsmaktens uppgifter.

5.2 Lagstiftning och andra handlingsmodeller i utlandet

5.2.1 Europeiska människorättskonventionen

I bedömningen av acceptansen för utfärdande av bestämmelser om befogenheter för militär underrättelseinhämtning innehas den största betydelsen i praktiken av Europeiska människorättskonventionen, som ingåtts år 1950 inom ramen för Europarådet (Europakonventionen; FördrS 63/1999) och till vilken Finland anslöt sig år 1989. 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 gäller underrättelseinhämtning som avser datatrafik eller därmed jämförbara former av myndighetsverksamhet.

Europadomstolens centrala avgörandepraxis med tanke på underrättelseverksamhet har bedömts i regeringens proposition med förslag till lag om militär underrättelseverksamhet (RP 203/2017 rd) och i regeringens proposition med förslag till lagstiftning om civil underrättelseinhämtning (RP 202/2017 rd). Nedan behandlas Europadomstolens praxis med fokus framför allt på Europadomstolens nyaste avgörandepraxis.

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 välbefinnande 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-postkorrespondens och annan elektronisk kommunikation som ska anses vara konfidentiell (bland annat 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 (bland annat 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 till exempel om 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 privatlivet, utan redan det att myndigheten samlar in och sparar uppgifter för senare

användning ska betraktas som ingripande (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 artikel 13 i Europakonventionen 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 privatlivet 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 godtycke som ingår i hemligt utövande av de verkställande befogenheterna ska kunna avvägras (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 (bland annat Kruslin mot Frankrike, Huvig mot Frankrike, Lambert mot Frankrike).

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 svarandestaternas 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 (bland annat Klass mot Tyskland, Weber och Saravia mot Tyskland). Den nationella säkerheten kan dock vara exponerad för många slags hot som det är svårt att förutse eller fastställa på förhand. Av detta följer att

klargörandet av begreppet nationell säkerhet 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 (bland annat 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.

Ovan beskrivna fall kan anses vara fall som baserar sig på Europadomstolens avgörandep Praxis, vilka återopas och utvecklas i Europadomstolens nyaste praxis. När det gäller Europadomstolens senare avgörandep Praxis kan man lyfta fram avgörandet i målet Roman Zakharov mot Ryssland, där Europadomstolen konstaterade att den hemliga underrättelseverksamheten hade kränkt de mänskliga rättigheterna. Klaganden framförde att tre telefonoperatörer hade kränkt skyddet för privatlivet. Bakgrunden till avgörandet var bland annat 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 vara garanterade 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.

I målet Big Brother Watch m.fl. mot Förenade kungariket prövade Europadomstolen Förenade kungarikets signalspaningssystem. Europadomstolen ansåg vidare att staterna har en omfattande prövningsrätt att besluta hurudant underrättelsesystem som är behövligt för att skydda den nationella säkerheten. Underrättelsesystemet överträdde i sig inte artikel 8 i Europakonventionen.

Domstolen ansåg dock att dess vanliga sätt att närma sig riktade signalspaningssystem, på grund av den moderna kommunikationsteknologins föränderliga natur, ska anpassas för att bättre beskriva dess särdrag, vilka omfattar såväl en risk för missbruk som ett berättigat behov av att hemlighålla verksamheten.

I synnerhet ett sådant system skulle underställa ändpunkt till ändpunkt-skyddsåtgärder, det vill säga att man på nationell nivå skulle göra en bedömning av åtgärdernas behovlighet och proportionalitet i fråga om varje fas i processen för att inhämta information i signalspaningen. Dessutom ska användningen av signalspaningssystemen underkastas en oberoende tillståndsprövning, i vilken operationens mål och omfattning ska framgå. Användningen av systemet ska även vara underkastad övervakning och en oberoende övervakning som görs i efterskott.

Således fastställde domstolen flera centrala kriterier, som skulle fastställas tydligt i en nationell lag innan ett sådant system kan anses stå i samklang med kraven i Europakonventionen. Genom att tillämpa dessa nya kriterier på Förenade kungarikets signalspaningssystem konstaterade domstolen att det fanns tre brister i Förenade kungarikets system. Ramarna ansågs utgöras av: 1) bristen på en oberoende fullmakt för signalspaningstillstånd, 2) de sökbegrepp som används i signalspaning och deras kategorier framgick inte av tillståndsansökan och 3) sökbegrepp och -kategorier som gäller en person behövde inte meddelas i tillståndsansökan.

Europadomstolen konstaterade att även om Förenade kungariket i sig hade en oberoende övervakare av verksamheten och ett rättsligt organ vars syfte är att undersöka klagomål som medborgarna lämnat in till det, var dessa dock inte tillräckliga. Europadomstolen ansåg att Förenade kungarikets lagstiftning bedömd som en helhet inte förmådde hålla inskränkningar i medborgarnas integritet på en nivå som är nödvändig i ett demokratiskt samhälle. Således ansågs Förenade kungariket bryta mot artikel 8 i Europakonventionen.

I målet Centrum för rättvisa mot Sverige var klaganden en svensk stiftelse, med uppgift att skydda individernas grundläggande fri- och rättigheter. Den stiftelse som utgjorde klagande åberopade att det varit möjligt att kapa och undersöka dess kommunikation genom signalspaning och att detta kan ske i framtiden. Klaganden åberopade att kommunikationen skedde dagligen per e-post, telefon och fax med personer och företag i Sverige och utomlands, ofta i vardagliga ärenden.

Stora sektionen konstaterade med en majoritet på femton röster (två emot) att en kränkning av artikel 8 i människorättskonventionen hade ägt rum. Den konstaterade särskilt att även om de centrala egenskaperna i det svenska omfattande signalspaningssystemet uppfyllde de krav som ställts på arten i lagen, fanns det dock tre brister i systemet: 1) det fanns inte någon klar regel för utplåning av material utan personuppgifter, 2) signalspaningslagen eller den övriga relevanta lagstiftningen förutsatte inte att individernas integritetsskydd beaktas vid beslut om förmedling av underrättelseinformation till utländska partner och 3) det fanns inte någon effektiv övervakning i efterskott. På grund av dessa brister uppfyllde systemet inte kravet på ändpunkt till ändpunkt-övervakning och det överskred den prövningsrätt som i detta hänseende lämnats till svarandestaten och som helhet skyddade det inte mot godtycke och risker för missbruk.

I sitt avgörande förhöll sig Europadomstolen sig inte absolut negativt till användning av så kallad massaövervakning (bulk interception regime). Europadomstolen anser att allvaret i de hot som avvärjs med den, förmågan hos personerna bakom hoten att agera utan att avslöjas i datanät och oförutsägbarheten för hur den elektroniska kommunikationen dirigeras motiverar att införandet av massaövervakning som har som mål att identifiera hot som äventyrar den nationella säkerheten hör till den nationella prövningsmarginalen. Europadomstolen har även mer generellt ansett att prövningsmarginalen är bred i valet av utbudet av metoder för att trygga den nationella säkerheten (bland annat Big Brother Watch punkt 275 och Centrum för Rättvisa punkt 365). Europadomstolen betonar dock att regleringen kring såväl riktade övervakningssystem som massaövervakningssystem i syfte att förhindra maktmissbruk ska uppfylla åtminstone ovan nämnda minimikrav.

Även i målet Centrum för Rättvisa mot Sverige (punkterna 239–245) konstaterar Europadomstolen att inskränkningen i skyddet för privatlivet enligt artikel 8 i Europakonventionen är av olika nivåer i de olika faserna av underrättelseinhämtning som avser datatrafik. Europadomstolen delar in processen i fyra faser: 1) inhämtande av datatrafik, 2) användning av sökbegrepp eller kategorier av sökbegrepp för selektering av datatrafik, 3) analys av filtrerad datatrafik och 4) lagring av data och framställande av en slutprodukt och användning av den. I början av processen ingriper inhämtandet av datatrafik, även om det täcker en stor grupp personer, inte i skyddet för en persons integritet i lika omfattande grad som i den tredje fasen, där en analytiker undersöker filtrerad kommunikation och anknutna uppgifter genom att kombinera sådana.

Europadomstolen riktar särskild uppmärksamhet även på att den svenska regleringen och det svenska systemet har bedömts konstant och vid behov förnyats även för att förbättra integritetsskyddet (punkt 351).

I målet ansåg Europadomstolen även att den i den svenska lagen föreskrivna möjligheten att samla in datatrafik för att utveckla signalspaningen befinner sig inom den nationella prövningsmarginalen (punkterna 291–293 i beslutet).

Det centrala i de mål som gäller Big Brother Watch och Centrum för Rättvisa är att Europadomstolen utvecklade sin rättspraxis kring de lagstiftningsmässiga förutsättningar som ställs på signalspaning (Big Brother Watch punkterna 343–361 och Centrum för Rättvisa punkterna 257–278); i stället för de sex krav som ska ställas på etablerad lagstiftning utifrån målet avseende Weber och Saravia (Weber och Saravia, punkt 95) förutsatte Europadomstolen att åtta krav uppfylls (Big Brother Watch punkt 361 och Centrum för Rättvisa punkt 275). Lagstiftning om signalspaning ska innehålla bestämmelser om 1) grunderna för att tillåta inhämtande av information, 2) de förhållanden där inhämtandet av information kan hänföra sig till en persons kommunikation, 3) förfarandet för att bevilja tillstånd, 4) de förfaranden som ska iaktas i valet, undersökningen och användningen av information, 5) de försiktighetsåtgärder som ska iaktas vid utlämnande av material till olika parter, 6) längden på en åtgärd, begränsningar av lagring av information och de förhållanden då information ska raderas och förstöras, 7) förfaranden och detaljerade bestämmelser med vilka den oberoende myndigheten övervakar att ovan nämnda garantier iakttagits och befogenheten för övervakaren att ingripa i lagstridig verksamhet samt 8) oberoende övervakning i efterskott och påföljder.

Effektiva rättsskyddsmedel (artikel 13)

Enligt artikel 13 i Europakonventionen ska var och en, vars i Europakonventionen 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. Underrättelseskyldigheten eller rätten för en person som är föremål för myndighetsåtgärder att få sin sak utredd har en väsentlig koppling till artikeln. Europadomstolens praxis beträffande artikel 13 i Europakonventionen har gått igenom i RP 203/2017 (s. 53–57) och i RP 202/2017, varför man i detta sammanhang hänvisar till de fall som presenterats i dessa på allmän nivå efter behov med fokus på Europadomstolens nyaste avgörandepaxis.

I fråga om artikel 8 i människorättskonventionen har Europadomstolen konstaterat att rättsskyddsmedlen ska vara så effektiva som möjligt, med beaktande av de begränsningar som orsakas av hemlig myndighetsverksamhets natur (Klass m.fl. mot Förbundsrepubliken Tyskland). Trots begränsningarna ansågs rättssäkerhetsgarantierna vara tillräckliga i ljuset av artikel 13, eftersom personen hade rätt att överföra sitt ärende för att behandlas av den kommission som övervakade verkställigheten och till den konstitutionella domstolen.

Ett rättsskyddsmedel är inte effektivt då den som söker ändring saknar den rätt som krävs för en överklagan (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

till exempel när klaganden av domstolen har fått ett föreläggande, som myndigheterna dock inte iakttar. När det på upprepat sätt kommit fram avsevärda dröjsmål i verkställandet av domar och beslut i vissa länder, har Europadomstolen i sin rättspraxis betonat att det nationella rättssystemet ska innehålla tillräckliga rättsskyddsgarantier även mot dröjsmål av denna typ.

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 åtgärd för inhämtande av information som har inriktats på personen. I fallen *Klass mot Tyskland* och *Weber och Saravia mot Tyskland* ansåg Europadomstolen att lagstiftning 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 Ekimdzhev mot Bulgarien* och *Dumitru Popescu mot Rumänien* konstaterade Europadomstolen att nationell lagstiftning 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 förutsatts i artikel 13 i Europakonventionen.

Förutsättningen ”nödvärdigt 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 åtgärder för inhämtande av information som inriktats på honom eller henne.

En förutsättning för att använda besvär- 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 årtal 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).

I sin nyare avgörandepraxis har Europadomstolen i målet beträffande Centrum för Rättvisa konstaterat att ett effektivt rättsskyddsmedel ska vara tillgängligt för alla som misstänker att de blivit ett objekt för hemliga myndighetsåtgärder. I fråga om riktade hemliga myndighetsåtgärder har Europadomstolen konstaterat att underrättelse i efterskott om en åtgärd till objektet erbjuder ett tillräckligt effektivt rättsskydd mot missbruk av åtgärderna. Å andra sidan har Europadomstolen även konstaterat att det kan vara tillräckligt med ett system där vem som helst som misstänker sig ha blivit objekt kan utöva rättsskyddsmedel oberoende av en underrättelse (Centrum för Rättvisa, punkt 271 och de i det hänvisade punkterna till målen Roman Zakharov mot Ryssland och Kennedy mot Förenade kungariket).

I målet beträffande Centrum för Rättvisa anser Europadomstolen att rättsskyddsmedel som inte är beroende av en underrättelse kan vara effektiva även i underrättelseinhämtning som avser datatrafik och att de beroende på förhållandena kan erbjuda bättre skydd för personen än rättsskyddsmedel som är bundna till en underrättelse (punkt 272 i målet). I synnerhet i en situation där hemliga myndighetsåtgärder riktar sig mot objekt utanför den ifrågavarande staten och personer utanför staten och även om identiteten i sig är känd, kan underrättelse om en åtgärd ha liten eller i praktiken inte någon betydelse överlag. I synnerhet om det inte finns information om personens vistelseort (punkt 272 i fallet).

Europadomstolen betonade vikten av att det finns självständiga organ som övervakar underrättelseverksamhet för systemets godtagbarhet. Det stora antalet rättsskyddsmekanismer kompenserar även att underrättelseåtgärder inte alltid meddelas till objekten. I fråga om övervakningssystemet riktar Europadomstolen i domen i målet beträffande Centrum för Rättvisa uppmärksamhet på oberoendet och det faktiska genomslaget för de anmärkningar som lagts fram i övervakningen.

I en situation där det inte finns någon underrättelseskyldighet, är det med tanke på rättsskyddsmedlets effektivt nödvändigt att det genomförs av en aktör som inte är beroende av myndigheten och som garanterar en rättvis handläggning och i mån av möjlighet erbjuder ett kontradiktoriskt förfarande. En sådan myndighets beslut ska motiveras och de ska vara juridiskt bindande bland annat i fråga om avslutande av olaglig avlyssning av kommunikation och förstöring av avlyssningsmaterial som inhämtats och/eller lagrats på olagligt sätt (punkt 273 i målet och målen Segerstedt-Wiberg m.fl. mot Sverige och Leander mot Sverige, till vilka det hänvisats i det målet).

I det svenska systemet har tillsynsombudsmannen en principiell skyldighet att närvara vid domstolsbehandlingen, tillträde till de handlingar som är relevanta för ärendet och rätt att yttra sig med anledning av dessa i domstolen. Enligt Europadomstolen kompenserar ett sådant arrangemang delvis begränsningarna av offentligheten för domstolsförfarandet och domstolsbesluten (punkterna 137–138 i målen).

I sin bedömning av den svenska lagstiftningen konstaterar Europadomstolen att den svenska tillsynsmyndigheten har behövliga befogenheter att övervaka signalspaningen i Sverige från början till slut. Tillsynsaktören kan göra en omfattande bedömning av signalspaningsmyndighetens verksamhet ur olika synvinklar, inbegripet inhämtningen,

analysen, användningen och utplåningen vad beträffar datatrafik. En annan central sak är att övervakare kan bedöma de använda sökbegreppen. Trots att övervakaren till vissa delar kan ge endast rekommendationer eller anvisningar (inte juridiskt bindande), ansåg Europadomstolen att övervakaren dock utöver detta har en möjlighet att avbryta verksamheten eller kräva att upptagningar och anteckningar ska förstöras. Dessa åtgärder hade även en juridiskt bindande karaktär. I fråga om de icke-juridiskt bindande rekommendationerna och anvisningarna konstaterade Europadomstolen att signalspaningsmyndigheten i praktiken alltid hade iakttagit dessa och i enskilda fall hade ärendet hänskjutits för att vidarebehandlas av regeringen (punkterna 347–350).

Europadomstolen konstaterade att den svenska tillsynsmyndigheten under åtta år gjort 102 granskningar och att den gör en årlig översikt (punkterna 351–352 i målet). Således konstaterade Europadomstolen att det inte hyser tvivel om att den svenska lagstiftningen och svensk praxis inte erbjuder en effektiv övervakning av signalspaning. Enligt Europadomstolen garanterar tillsynsmyndighetens roll i kombination med att även den deltar även i bedömningen av ärenden innan beslutfattandet en fungerande rättsskyddsgaranti mot godtycklighet av myndigheten i fråga om signalspaning (punkt 353 i målet).

I sin bedömning av målet beträffande Centrum för Rättvisa konstaterar Europadomstolen att rättsskyddsmedel som inte är beroende av en underrättelse ska vara tillgängliga för dem som misstänker att de blivit föremål för en åtgärd (punkt 355 i målet). Europadomstolen konstaterar att den svenska lagstiftningen gav personerna en möjlighet att överföra sin sak för prövning (punkt 356 i målet). Europadomstolen konstaterade dock att de behöriga övervakningsorganet (SIUN) i det svenska systemet beviljar även tillstånd till underrättelseinhämtning som avser datatrafik. Således kunde den myndighet som genomför övervakningen i efterskott och tillgodoser rättsskyddet för den enskilde inte anses vara särskilt objektiv eller att dess behandling var grundlig. Även frågan om en intressekonflikt blir aktuell, vilket kan locka till generell behandling av det behandlade ärendet (punkt 359). Dock även SIUN även föremål för extern övervakning, men en sådan övervakning hade i praktiken inte gjorts och en sådana lagstadgad uppgift hade inte heller egentligen föreskrivit (punkt 360 i målet).

Europadomstolen ansåg att SIUN:s dubbelroll försvagade övervakningen av underrättelseinhämtning som avser datatrafik i den mån att den orsakar risker för tillgodoseendet av de grundläggande fri- och rättigheterna för de berörda personerna (punkt 372 i målet). Delvis även på grund av detta ansåg Europadomstolen att den svenska lagstiftningen inte uppfyllde kraven i artikel 8 i Europakonventionen (punkt 373 i målet).

5.2.2 Konventionen om medborgerliga och politiska rättigheter

Artikel 17 i konventionen om medborgerliga och politiska rättigheter (MP-konventionen, FördrS 7–8/1976) innehåller bestämmelser bland annat om skyddet för kommunikation. Enligt punkt 1 i artikeln får ingen utsättas för godtyckligt eller olagligt ingripande med avseende på privatliv, familj, hem eller korrespondens och inte heller för olagliga angrepp på sin heder eller sitt anseende. Enligt punkt 2 i artikeln har var och en rätt till lagens skydd mot sådana ingripanden och angrepp. I artikel 2.1 i MP-konventionen ställs en skyldighet för konventionsstaterna att vidta åtgärder för att skydda de rättigheter som tryggats i konventionen, inklusive rättigheterna i artikel 17.

Det finns bestämmelser om skyddet för privatlivet även i andra människorättskonventioner av FN, såsom konventionen om barnets rättigheter (FördrS 59 och 60/1991), vars artikel 16 innehåller bestämmelser om barnets rätt till skydd för integritet, familj, hem och brevväxling, och konventionen om rättigheter för personer med funktionsnedsättning (FördrS 26 och

27/2016), vars artikel 22 innehåller bestämmelser om skyddet för integritet, familj, hem och brevväxling för personer med funktionsnedsättning.

FN:s människorättskommittén som övervakar genomförandet av MP-konventionen har gett tolkningsståndpunkter om artikel 17, som gäller skyddet för privatlivet. I människorättskommitténs allmänna ståndpunkt om artikeln (General Comment no. 16, 8.4.1988) har denna bestämmelse i konventionen tolkats innehålla en skyldighet för staten själv att avhålla sig från åtgärder i strid med artikel 17 och därtill att ingripa i kränkningar av företag genom lagstiftningsmässiga metoder. Uttrycket ”brevväxling” i artikeln innebär bland annat olika former av kommunikation, såsom telefonsamtal och e-post. Alla former av avbrytande av privat kommunikation, censur, granskningar eller offentliggörande innebär ett ingrepp i brevväxlingen.

I artikel 17 i konventionen uppräknas inte grunderna för att begränsa de rättigheter som tryggas i artikeln. I artikeln förbjuds uttryckligen endast godtyckliga och olagliga inskränkningar av rättigheterna. Målet med förbudet mot godtyckliga inskränkningar är att även lagbaserade inskränkningar ska vara förenliga med föreskrifterna och ändamålen i MP-konventionen och skäligen i respektive fall. Enligt rättslitteraturen finns det hjälp för att tolka vad som är godtagbara begränsningsgrunder i kriterierna för att göra begränsningar som gäller de andra artiklarna i MP-konventionen och de begränsningsgrunder som avses i artikel 8 i Europakonventionen.

Enligt artikel 4 i MP-konventionen är det möjligt att avvika från ett konventionsåtagande endast vid ett allmänt nödläge som hotar nationens fortbestånd. Ett sådant nödläge ska officiellt ha utlysts som ett sådant. I så fall kan konventionsstaterna vidta åtgärder som innebär en avvikelse från deras skyldigheter enligt MP-konventionen i den omfattning som situationen förutsätter det. En ytterligare förutsättning är att dessa åtgärder inte strider mot landets övriga åtaganden enligt den internationella rätten och inte innebär diskriminering enbart på grund av ras, hudfärg, kön, språk, religion eller social härkomst.

FN:s människorättskommitté, som övervakar genomförandet av MP-konventionen har i sina slutsatser från år 2021 beträffande Finland (CCPR/C/FIN/CO/7) uppmanat konventionsstaten att säkerställa att (a) all övervakning och allt ingripande i privatlivet, både av civila och militära aktörer, såsom nätövervakning, teleavlyssning, inhämtning av uppgifter om kommunikation och informationssökning, regleras genom ändamålsenlig lagstiftning som överensstämmer med konventionen, i synnerhet artikel 17, inbegripet laglighets-, proportionalitets- och nödvändighetsprinciperna; och att (b) det för övervakning och teleavlyssning krävs tillstånd av domstol, att dessa aktiviteter övervakas med hjälp av effektiva och oberoende system och att de personer som är föremål för aktiviteterna har tillgång till effektiva rättsmedel på tillbörligt sätt i det fall att deras rättigheter kränks.

FN:s människorättsråd har godkänt flera rapporter om skyddet för privatlivet under digitaliseringseran (A/HRC/27/37 (2014), A/HRC/39/29 (2018), A/HRC/48/31 (2021) och A/HRC/51/17(2022)). FN:s människorättsråd har även riktat uppmärksamhet på säkerställande av källskyddet i sin resolution om journalisternas säkerhet (A/HRC/RES/51/9 (2022)).

5.2.3 Unionsrätten

Bestämmelserna i EU:s stadga om de grundläggande rättigheterna (EUT C 326, 26.10.2012) gäller enligt artikel 51.1 i stadgan med beaktande av subsidiaritetsprincipen, unionens institutioner, organ och byråer samt medlemsstaterna endast när dessa tillämpar

unionsrätten. EU:s stadga om de grundläggande rättigheterna tillämpas således inte i situationer som handlar endast om tillämpningen av den nationella lagen och som inte regleras i EU-rätten. Även utanför tillämpningsområdet för EU-rätten är det möjligt att få tolkningshjälp från stadgan om grundläggande rättigheter till exempel i situationer där Europadomstolen inte behandlat någon rättighet eller anknuten fråga om vilken det finns rättspraxis från EU-domstolen.

Enligt artikel 7 i stadgan om de grundläggande rättigheterna 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 första stycket i artikeln 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 tredje stycket i samma artikel 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 avgörandep Praxis avseende artikel 8 i människorättskonventionen ska således anses vara relevant även för tolkningen av artikel 7 i stadgan om de grundläggande friheterna (utlåtande om EU:s anslutning till Europakonventionen, 2/13, EU:C:2014:2454, 170 punkten; dom Kadi och Al Barakat, C-402/05 och C-415/04 P, 281–285 punkten; dom Internationale Handelsgesellschaft, C-11/70, 4 punkten).

I samband med underrättelselagstiftningen är de undantag som ingår i EU-lagstiftningen av relevans, utifrån vilka tillämpningen av EU-rätten i flera rättsakter har avgränsats utanför ärenden som gäller den nationella säkerheten. Undantagen baserar sig på artikel 4.2 i fördraget om Europeiska unionen, enligt vilken i synnerhet den nationella säkerheten ska vara varje medlemsstats eget ansvar. Unionen har således ingen behörighet när det gäller nationell säkerhet. Det är dock inte alltid i praktiken entydigt att tillämpningsområdet för EU-rätten inte gäller utifrån det undantag som gäller den nationella säkerheten. EU:s rättsordning och vissa förhandsavgöranden av EU-domstolen och talan om ogiltigförklaring i EU-lagstiftningen är således av betydelse även för underrättelsekommittén och utvecklingen av den nationella lagstiftningen om den. En medlemsstat som åberopar en grund som gäller den nationella säkerheten ska påvisa behovet av att förlita sig på den aktuella grunden (dom ZZ, C-300/11; dom Insinööritoimisto InsTiimi Oy, C-615/10, 35 punkten; dom kommissionen mot Finland, C-284/05, 45 och 47 punkten).

Undantaget kan dock inte anses vara absolut, utan underrättelsemyndigheternas verksamhet kan i vissa situationer omfattas av EU-rättens räckvidd och således omfattas av EU:s reglering kring

grundläggande fri- och rättigheter som ett komplement till de rättigheter som tryggas i nationella konstitutionella bestämmelserna och de internationella människorättskonventionerna. Det undantag som gäller den nationella säkerheten är således inte ett alltomfattande undantag och utesluter i sig inte helt tillämpligheten för unionsrätten.

Unionsdomstolen har sedermera styrkt denna slutsats genom att konstatera att åberopande av den nationella säkerheten inte berättigar till att kringgå unionsrätten, inbegripet den övervakning som baserar sig på Europeiska unionens stadga om de grundläggande rättigheterna. Domstolen har förtydligat principen i anknytning till medlemsstaternas arrangemang, där man allmänt och utan åtskillnad har ålagt teleoperatörerna att lagra uppgifter om kommunikation och ordna tillgång till dessa i realtid för underrättelsemyndigheterna för att skydda den nationella säkerheten. Domstolen har även definierat den nationella säkerheten som skydd av statens vitala funktioner och samhällets grundläggande intresse samt skydd mot att statens grundstrukturer rubbas och att befolkningen hotas (EU-domstolen, de kombinerande målen C-511/18, C-512/18 och C-520/18 punkterna 99 och 135).

De så kallade data retention-regleringen ska anses ha det närmaste sambandet med tanke på underrättelseverksamhet. EU-domstolens rättspraxis om dataskyddsdirektivet för elektronisk kommunikation utvecklas hela tiden. Efter Tele2 Sverige -domen har förvaring och användning av plats- och trafikuppgifter bedömts åtminstone i följande avgöranden: dom Ministerio Fiscal, C-207/16; dom Privacy International, C-623/17; dom La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18; dom Prokuratuur, C-746/18; dom SpaceNet, C-793/19 och C-794/19; dom Commissioner of An Garda Síochána, C-140/20; dom VD och SR, C-339/20 och C-397/20; dom Spetsializirana prokuratura, C-350/21; dom A. G. och Lietuvos Respublikos generalinė prokuratūra, C-162/22; dom La Quadrature du Net m.fl., C-470/21; dom Procura della Repubblica presso il Tribunale di Bolzano, C-178/22. EU-domstolens tolkningspraxis har påverkat behandlingen av personuppgifter i anknytning till bekämpning av brott. I dessa sammanhang har EU-domstolen även tolkat artikel 7 om skyddet för hemligheten i fråga om förtroliga meddelanden och artikel 8 om skyddet för personuppgifter i grundstadgan. Unionsdomstolen har ansett att ett nationellt regelverk, enligt vilket leverantörer av elektroniska kommunikationstjänster ska förvara trafik- och platsuppgifter för att skydda den nationella säkerheten och bekämpa brottslighet omfattas av tillämpningsområdet för direktiv 2002/58 (dom La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, punkterna 100–104 och dom Lietuvos Respublikos generalinė prokuratūra, C-162/22, punkt 28).

I unionsdomstolens rättspraxis konstateras att ”när medlemsstaterna genomför åtgärder som innebär undantag från konfidentialiteten vid elektronisk kommunikation, utan att ålägga tjänsteleverantörer av sådan kommunikation någon skyldighet att behandla uppgifter, omfattas skyddet av de berörda personernas uppgifter inte av direktivet om integritet och elektronisk kommunikation utan endast nationell rätt”. Det handlar dock inte om en sådan situation eftersom ”all behandling av personuppgifter av leverantörer av elektroniska kommunikationstjänster omfattas av tillämpningsområdet [för direktivet om integritet och elektronisk kommunikation], inbegripet behandling som följer av skyldigheter som ställts av myndigheterna för dem” (dom 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, EU:C:2020:791, 101 punkten).

Däremot kan det ingrepp i de grundläggande rättigheterna enligt artiklarna 7 och 8 i stadgan som är följden av myndigheters åtkomst till uppgifter om fysisk identitet som lagras av leverantörer av elektroniska kommunikationstjänster, utan att dessa uppgifter kan kopplas till information om utförda kommunikationer, inte anses som allvarligt, eftersom dessa uppgifter sedda som en helhet inte gör det möjligt att dra några precisa slutsatser om privatlivet för de personer vilkas uppgifter berörs. Denna åtkomst kan därför motiveras av ändamålet att

förebygga, undersöka, avslöja och lagföra brott i allmänhet (se, för ett liknande resonemang, dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkterna 54, 57 och 60).

EU-domstolen har även ansett att man i domstolens etablerade rättspraxis styrkt principen om att den nationella säkerheten, inbegripet landets försvar, är ett mål enligt ett allmänt intresse och att den nationella säkerheten är en betydelsefullare begränsningsgrund än brottsbekämpning (se dom av den 30 april 2024, La Quadrature du net m.fl., C470/21, punkt 97 och på motsvarande sätt dom av den 6 oktober 2020 La Quadrature du Net m.fl. (C-511/18, C-512/18 och C-520/18, EU:C:2020:791, punkt 166).

Vissa omständigheter i underrättelsemyndigheternas verksamhet, såsom inhämtande av information som hänför sig till datatrafik, ligger överlag utanför unionsrättens räckvidd. EU-domstolen har även betonat att inhämtande av information som ska hemlighållas och befinner sig utanför unionsrättens räckvidd, dock ska uppfylla de krav som Europakonventionen ställer.

I sin rättspraxis avseende dataskydd har EU-domstolen riktat uppmärksamhet på bland annat övervakningen av det arrangemang som är föremål för bedömning, de tillgängliga rättsmedlen, lämnande av uppgifter och dataskyddet samt personkretsen, förhandstillståndet, tillgången till information, förvaringstiden för uppgifter och förutsättningar för att radera uppgifter (se dom Tele2 Sverige, C-203/15 och C-698/15, 106–111, 117–119, 120–122 punkten; dom WebMind, C-419/14, 77–78 punkten; dom Schrems, C-362/14, 40 och 95 punkten; dom Digital Rights Ireland, C-293/12 och C-594/12, 56–67 punkten; dom UGT-Rioja m.fl., C-428/06 – C-434/06, 80 punkten). I synnerhet i fråga om brottsbekämpning har EU-domstolen riktat uppmärksamhet på att tillgången till en mobiltelefons uppgifter kan täcka innehållet i kommunikationen och förmedlingsuppgifter, men därtill även fotografier och bläddringshistoriken på internet. Genom tillgången till en sådan samling av uppgifter

går det enligt domstolen att i vissa fall dra mycket precisa slutsatser om den registrerades privatliv, såsom personens dagliga vanor, stadigvarande eller tillfälliga bostadsort, dagliga eller allmänna rörelsemönster, aktiviteter, sociala kontakter och umgängeskretsar. Således har unionsdomstolen konstaterat att om en myndighet bereder sig tillgång till uppgifterna i en

mobiltelefon, är det frågan om ett allvarligt, eller till och med synnerligen allvarligt ingrepp i de grundläggande rättigheter som fastslås i artiklarna 7 och 8 i stadgan om de grundläggande rättigheterna (dom Bezirkshauptmannschaft Landeck, C-548/21, punkterna 92–93, 95).

Sammanfattningsvis är det utifrån de domar till vilka det hänvisats ovan möjligt att dra en slutsats om att den nationella säkerheten, inklusive landets försvar, har en högre ställning än brottsbekämpningen i rättsobjektens hierarki. Således ligger den även längre bort från tillämpningen av Europeiska unionens stadga om de grundläggande rättigheterna. Dessutom kan det konstateras att de uppgifter som ska lagras och behandlingen av dessa ska bedömas utifrån hur djupgående slutsatser det är möjligt att göra utifrån dessa i fråga om en privatpersons liv och således hur de facto ingriper i skyddet för personens privatliv.

5.2.4 Utländsk lagstiftning

5.2.4.1 Sverige

Allmänt

Militär underrättelseverksamhet bedrivs av Militära underrättelse- och säkerhetstjänsten, MUST, Försvarets radioanstalt, FRA, Försvarets materielverk, FMV, och Totalförsvarets forskningsinstitut, FOI.

I Sverige styrs signalspaningen i försvarsunderrättelseverksamheten av lagen om signalspaning i försvarsunderrättelseverksamhet, 2008:717) och förordningen om signalspaning i försvarsunderrättelseverksamhet 2008:923, som kompletterar lagen. Försvarets radioanstalt, FRA, fungerar som nationell signalspaningsmyndighet.

Enligt signalspaningslagen avses med signalspaning inhämtning av signaler i elektronisk form. Definitionen är teknikneutral och täcker alla metoder för signalspaning, såsom till exempel tråd- och radiosignalspaning samt manuell och automatiserad informationsinhämtning. 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. Förbudet gäller dock inte signaler som överförs självständigt mellan tekniska system då signalerna inte innehåller personuppgifter eller då signalerna sänds till utländsk militär personal, utländska statliga fartyg, statliga luftfartyg eller militära rådgivare eller då kommer från motsvarande aktörer från utlandet.

Slutbetänkandet Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (SOU 2024:59) har färdigställts hösten 2024 i Sverige beträffande revidering av lagen om signalspaning i försvarsunderrättelseverksamhet. I betänkandet har man bland annat föreslagit ett särskilt undantag till förbudet att inhämta inrikes trafik, om sådan spaning är betydelsefull för att bekämpa externa hot mot den svenska säkerheten. Målet med förslaget är att säkerställa att det i krigsförhållanden är möjligt att utöva signalspaning mot fientlig verksamhet som bedrivs i Sverige och som hotar Sveriges suveränitet och territoriella integritet, även från icke militära källor. I betänkandet har man dessutom föreslagit att 1 § i signalspaningslagen ändras på så sätt att det är möjligt att inhämta signaler oavsett om signalerna är under förmedling eller är lagrade. Signalerna kan vara lagrade till exempel i nätanslutna anordningar eller program.¹⁰

Ett utkast till proposition har sänts på remiss i Sverige i juli 2025 (Fö2024/01478)¹¹, vilket beaktar vad som angetts i slutbetänkandet (SOU 2024:59), men även innehåller förslag om nya ändringar för att uppdatera underrättelselagarna. Den föreslagna nya lagen och lagändringarna träder i kraft i juni 2026 enligt förslaget. Utredningen innehåller ett utkast till regeringsproposition till en ny lag om signalspaning i underrättelseverksamhet vid försvarsmakten under krig eller vid hot om krig. Dessutom föreslås ändringar i lagen om

¹⁰ SOU 2024:59; s. 241.

¹¹ Fö2024:01478 Utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (<https://www.regeringen.se/contentassets/20faf90d0b7c40ba82a37dd85db22bf0/utkast-lagratsremiss-signalspaning-i-forsvarsunderrattelseverksamhet---en-modern-och-andamalsenlig-lagstiftning.pdf>).

signalspaning i försvarsunderrättelseverksamhet och i lagar med samband med den. Det föreslås att signalspaningslagen ändras bland annat på så sätt att signalspaning är möjligt även i vid repetitionsövningar.

Sökbegreppen i underrättelseinhämtning som avser datatrafik

I 1 § 3 mom. i den svenska signalspaningslagen föreskrivs att om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

Enligt förarbetena till lagen (Prop. 2006/07:63) används sådana underrättelser endast för att utveckla underrättelsemyndighetens tekniska kompetens, för att ännu bättre kunna utföra underrättelseuppdrag. Av inhämtningen av tekniska uppgifter och behandlingen av tekniska uppgifter uppkommer således inte sådana underrättelser som utnyttjas för att utföra underrättelseuppdrag. I förarbetena till lagen konstateras därtill att sådan uppnådd teknisk kompetens och information om sådan kan delas mellan myndigheterna. Den information som delas är inte egentliga underrättelser, och inte kommunikation som omfattas av skyddet för privatlivet.

Enligt 3 § i signalspaningslagen får inhämtning av signaler basera sig endast på använda sökbegrepp. Integritetsskyddet ska beaktas då sökbegreppen fastställs och används. Sökbegrepp som direkt hänför sig till en viss fysisk person får användas endast om det är synnerligen viktigt för verksamheten. Sökbegreppen kan beskriva representationer för de aktörer, organisationer, plattformar eller tekniska system till vilka signalspaningen ska hänföra sig. Sökbegreppen möjliggör tekniskt sett att den väsentliga informationen hittas och identifieras. Ett enskilt sökbegrepp kan ofta gälla en viss kommunikationstjänst som målet använder, till exempel en viss mobiltjänst eller e-posttjänst.¹² I förarbetena till lagen¹³ konstateras att den snabbt föränderliga signalmiljön förutsätter att även sökbegreppen redigeras och fastställa då ny information flyter in.

Enligt 3 § i förordningen om signalspaning i försvarsunderrättelseverksamhet ska FRA till Statens inspektion för försvarsunderrättelseverksamheten (SIUN) redovisa sådana sökbegrepp som är direkt hänförliga till fysisk person och som används i signalspaningsverksamheten.

Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik

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.

Förordningen om signalspaning i försvarsunderrättelseverksamhet 2008:923 har ändrats genom den förordning som trädde i kraft den 1 januari 2025 (SFS 2024:427). Genom

¹² SOU 2024:59, s. 56.

¹³ Prop. 2006/07:63, s. 77–78.

ändringsförordningen har man preciserat skyldigheten att utplåna vissa upptagningar som avses i signalspaningslagen. Upptagningar och anteckningar ska utplånas på så sätt att de inte kan återskapas.

Enligt 2 kap. 19 § i lagen om behandling av personer uppgifter vid FRA (Lag (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt) får personuppgifter inte behandlas längre än vad som behövs för behandlingens syften.

Enligt 3 kap. 1 § i förordningen (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt får det vid Försvarets radioanstalt finnas uppgiftssamlingar för råmaterial som innehåller personuppgifter och obearbetat och automatiskt bearbetat material vars relevans för verksamheten ännu inte har bedömts. Personuppgifter som ingår i sådan rådata får dock inte behandlas längre än i ett år från det att behandlingen av uppgifter har inletts.

Underrättelseskyldigheten

Signalspaningslagens 11 a § förutsätter att en underrättelse ska lämnas till en fysisk person så snart det kan ske, dock senast en månad efter att det inhämtningsuppdrag som föranlett inhämtningen avslutades och om när inhämtningen skett och syftet med inhämtningen. Enligt 11 b § i lagen får underrättelsen skjutas upp, om sekretess hindrar att underrättelsen lämnas. Har det på grund av sekretess inte kunnat lämnas någon underrättelse inom ett år från det att inhämtningsuppdraget avslutades, behöver någon underrättelse inte lämnas. En underrättelse ska inte heller lämnas om inhämtningen uteslutande avser främmande makts förhållanden eller förhållanden mellan främmande makter.

I Sverige föreslås att ovan nämnda underrättelseskyldighet slopas. I propositionen har man beaktat Europadomstolens ställningstagande i målet beträffande Centrum för Rättvisa. I utkastet till proposition¹⁴ konstateras att FRA utifrån sekretessgrunden aldrig gett underrättelser utifrån 11 a § och att det inte heller framöver är sannolikt att underrättelser ges. Enligt utkastet till proposition är underrättelseskyldigheten inte av betydelse som garant för rättsskyddet eller integritetsskyddet. Kontrollskyldigheten enligt 10 a § i signalspaningslagen fullgör detta syfte.

5.2.4.2 Norge

Allmänt

Den norska utrikes underrättelsetjänsten utgörs av Etterretningstjenesten (E-tjenesten), vars uppgifter och befogenheter föreskrivs i lagen om underrättelsetjänsten (Lov om Etterretningstjenesten). Den nuvarande norska lagen om underrättelsetjänsten har trätt i kraft år 2021.

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 separat förordning (Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste).

¹⁴ Fö2024/01478, Utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning, s. 124–126.

Sökbegreppen i underrättelseinhämtning som avser datatrafik

Enligt 5 kap. 3 § i lagen om underrättelsetjänsten kan underrättelsetjänsten inhämta rådata i massaform (raw data in bulk), då det behövs för att få ett relevant och tillräckligt informationsunderlag. Sökningar i sådan rådata ska uppfylla de grundläggande förutsättningarna för riktad underrättelseinhämtning och sökprocessen ska registreras för kontrollen. Sökningar i rådata vilka gäller en person som vistas i Norge får göras endast då det är absolut nödvändigt för att utföra uppdrag enligt 3 kap. 1 § i lagen om underrättelsetjänsten. Begränsningen gäller inte för utländska personer eller personer utan medborgarskap, som agerar för en främmande stat eller en instans som påminner om en statlig aktör.

Enligt 7 kap. 5 § i lagen om underrättelsetjänsten kan underrättelsetjänsten göra testinhämtningar och testanalyser i gränsöverskridande elektronisk datatrafik och gränsöverskridande nät. Enligt paragrafen får testinhämtning och testanalyser användas endast för att möjliggöra val, filtrering, lagring, sökning, ombearbetning, förståelse för signalmiljön, tjänster och identifiering av dataformat samt för annat tekniskt stöd.

En testinhämtning görs genom plockning från ofiltrerad datatrafik eller från flera datatrafikflöden. En plockning får inte överstiga 30 sekunder och högst en plockning per timme får göras. Plockningar får inte sparas längre än vad som behövs och de ska raderas senast inom 14 dagar. Plockningarna ska lagras i ett kortvarigt förvar, som ska hållas åtskilt från de förvar som är reserverade för sparad metadata och sparade innehållsuppgifter.

Enligt 7 kap. 7 § i den norska lagen om underrättelsetjänsten kan underrättelsetjänsten inhämta och spara metadata i massaform (metadata in bulk) från elektronisk kommunikation som går över den norska gränsen. I 6 § i 7 kap. i lagen finns det dock bestämmelser om skyldigheten att försöka förebygga att man lagrar sådan metadata som gäller kommunikation mellan parter som vistas i Norge. Enligt 7 § i lagen avses med metadata uppgifter som beskriver annan data eller innehåller tilläggsuppgifter i anknytning till data, såsom uppgifter som beskriver innehållets form, avsändare och mottagare eller kommunikationens omfattning, position, tidpunkt och längd. För att förebygga att innehållsuppgifter lagras ska underrättelsetjänsten föra en förteckning över de typer av metadata som kan lagras och förteckningen ska vara tillgänglig för tillsynsmyndigheterna.

Enligt 8 § i 7 kap. är det möjligt att i lagrad metadata göra sökningar som baserar sig på sökbegrepp med domstolstillstånd. Sökningar i lagrad metadata kan göras endast av personer som utbildats och utsetts för denna uppgift. Enligt 5 § i lagen får uppdatering, teknisk analys och felsökning göras i lagrad metadata endast av sådana tekniska experter som inte arbetar med uppgifter inom underrättelseanalys.

Enligt 7 kap. 9 § i den norska lagen om underrättelsetjänsten kan underrättelsetjänsten dessutom med domstolstillstånd inhämta och lagra innehållsuppgifter och anknuten metadata från sådan datatrafik som överskrider den norska gränsen. Definitionen av innehållsuppgifter att det handlar om uppgifter som inte utgör metadata.

Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik

Tekniska parametrar och behandlade testanalyser vilka inte kan förenas med enskilda personer kan sparas så länge som det behövs för att uppnå målen med testanalyser enligt 7 kap. 5 § i lagen.

Enligt 7 kap. 7 § i lagen om underrättelsetjänsten ska lagrad metadata raderas senast inom 18 månader.

Underrättelseskyldigheten

Den norska lagen om underrättelsetjänsten innehåller inte bestämmelser om någon allmän skyldighet för myndigheten att ge en underrättelse om att en person varit föremål för underrättelseinhämtning. Användningen av metoder för underrättelseinhämtning övervakas av utskottet för kontroll av underrättelseinhämtning (EOS-utvalget). Det är möjligt att överklaga till utskottet för kontroll av underrättelseinhämtning, om man misstänker att man varit föremål för underrättelseinhämtning eller att egna uppgifter behandlats lagstridigt. I enlighet med 8 § i EOS-kontrollagen (Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste) har utskottet för kontroll av underrättelseinhämtning bred tillgång till underrättelsetjänsternas uppgifter i sin kontrolluppgift. I princip innehåller ett utlåtande med anledning av en överklagan dock i princip inte något ställningstagande till om personen varit föremål för underrättelseinhämtning, eftersom det handlar om sekretessbelagd information.

5.2.4.3 Danmark

Allmänt

I Danmark ansvarar försvarsmaktens underrättelsetjänst FE (Forsvarets Efterretningstjeneste) för underrättelseinhämtning utomlands. Lagen om försvarsmaktens underrättelsetjänst (Lov om Forsvarets Efterretningstjeneste, nedan FE-lagen) innehåller bestämmelser om underrättelsetjänstens uppgifter, befogenheter och övervakningen av dess verksamhet. En proposition om ändring av FE-lagen har varit på remiss i februari 2025.¹⁵ Försvarsministeriet har i april 2025 meddelat att lagpropositionen skjuts upp till nästa år.¹⁶ Bakgrunden till ändringsförslaget utgörs av Europadomstolens avgörandepraxis och behovet av att uppdatera FE-lagen så att den ligger i linje med domstolens avgörandepraxis.

Sökbegreppen i underrättelseinhämtning som avser datatrafik

Den danska FE-lagen innehåller inte särskilda bestämmelser om fastställande av sökbegrepp och teknisk analys för att upptäcka ändringar i signalmiljön.

Utplåning av information

Enligt 6 § 1 mom. i FE-lagen ska försvarsmaktens underrättelsetjänst i princip radera uppgifter om fysiska eller juridiska personer med hemvist i Danmark, vilka har inhämtats i samband med verksamhet enligt 1 § 1 mom., om man under de senaste 15 åren inte inhämtat ny innehållsmässig information om samma ärende och andra bestämmelser inte utfärdats annanstans. Enligt paragrafens 2 mom. ska rådata raderas inom 15 år från inhämtningstidpunkten. Det är dock möjligt att avvika från detta, om det finns väsentliga skäl för detta med tanke på skötseln av uppgifter. Enligt 6 a § i FE-lagen ska inhämtade uppgifter dock raderas oberoende av om lagringstiden gått ut, om ärendena eller handlingarna inte längre uppfyller villkoren för behandling av uppgifter. En myndighet har inte någon skyldighet att

¹⁵ <https://hoeringsportalen.dk/Hearing/Details/69633>

¹⁶ <https://www.ft.dk/samling/20241/almindel/FOU/bilag/127/3012501.pdf>

kontinuerligt granska uppgifter för att bedöma om de förutsättningar som ställs i 4 och 5 § för behandling av personuppgifter fortfarande föreligger.

Underrättelseskyldigheten

FE-lagen innehåller inte bestämmelser om någon allmän skyldighet för myndigheten att göra en underrättelse om att en person varit föremål för underrättelseinhämtning. Om man misstänker att man varit föremål för underrättelseinhämtning är det möjligt att göra en underrättelse till myndigheten för tillsyn över underrättelsetjänsterna (Tilsynet med Efterretningstjenesterne, nedan TET).

5.2.4.4 Tyskland

Allmänt

Bundesnachrichtendienst (BND) är Tysklands underrättelsetjänst för utlandet och ansvarar för extern informationsinhämtning gällande såväl civila som militära hot. Uppgifterna inom säkerhetstjänsten för inrikesärenden har delats upp på så sätt att Bundesamt für Verfassungsschutz (BfV) fungerar som civil säkerhetstjänst och Militärischer Abschirmsdienst (MAD) som militär säkerhetstjänst. MAD:s primära uppgift är att upptäcka och bekämpa sådana hot som väller fram från insidan av den tyska försvarsförvaltningen. Uppgifterna och befogenheterna för alla ovan nämnda aktörer föreskrivs i separata lagar, även om lagarna om BND:s och MAD:s verksamhet i fråga om befogenheter i stor utsträckning innehåller hänvisningar till lagen om BfV:s verksamhet, vilken reglerar samarbetet mellan förbundsrepublikens och delstaternas säkerhetstjänster (Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, nedan BfV-lagen).

Lagen om underrättelsetjänsten för utrikesärenden (nedan BND-lagen) har förnyats som en följd av grundlagsdomstolens beslut från maj 2020¹⁷. Den reviderade BND-lagen trädde i kraft den 1 januari 2022. I reformen beaktades i synnerhet tillgodoseendet av integritetsskyddet och pressfriheten i underrättelseinhämtning i utländsk datatrafik.

Lagen om begränsning av post- och telesekretessen (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, nedan G10-lagen) är dessutom av betydelse för befogenhetsregleringen. Den innehåller reglering som gäller alla sådana metoder för underrättelseinhämtning med vilka säkerhets- och underrättelsetjänsternas underrättelseinhämtning ingriper i innehållet i förtroliga meddelanden.

Sökbegreppen i underrättelseinhämtning som avser datatrafik

I 19 § i BND-lagen finns det bestämmelser om strategisk underrättelseinhämtning i utländsk datatrafik. Enligt 8 mom. i paragrafen är obegränsad underrättelseinhämtning som avser datatrafik förbjuden och därtill får inhämtningen rikta sig på högst 30 procent av de existerande datatrafiknäten. Enligt paragrafens 5 mom. är det tillåtet att genomföra inhämtningen endast utifrån sökbegrepp. Sökbegreppen ska bland annat ha fastställts i förväg. Enligt 7 mom. i

¹⁷ Bundesverfassungsgericht, 1 BvR 2835/17 (19.5.2020), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html

paragrafen får underrättelseinhämtning inte hänföra sig till tyskar, personer som vistas i Tyskland eller inhemska juridiska personer.

G10-lagens 5 § behandlar begränsning av den grundlagstryggade meddelandehemligheten i underrättelseinhämtning som avser datatrafik. Enligt bestämmelsen får BND med tillstånd av det parlamentariska tillsynsutskottet genomföra underrättelseinhämtning som avser datatrafik, om det är nödvändigt för att upptäcka och förebygga vissa hot. Enligt paragrafens 2 mom. är det inte tillåtet att använda sökbegrepp som leder till riktad uppföljning av enskilda teletrafikförbindelser eller som gäller kärnområdet i skyddet för privatlivet.

Utplåning av information

BND-lagens 27 § innehåller bestämmelser om värdering av inhämtade uppgifter skyldigheten att granska dessa. Inhämtade uppgifter ska granskas utan dröjsmål och därefter regelbundet, med minst sju års mellanrum, för att utreda om de ensamma eller tillsammans med redan existerande uppgifter behövs för de syften som fastställts i 19 § 1 mom. Om personuppgifter inte behövs för dessa syften, ska de raderas utan dröjsmål.

Enligt BND-lagens 36 § ska man utan dröjsmål radera och dokumentera raderingen av uppgifter som gäller kärnområdet i privatlivet och som eventuellt fås i samband med underrättelseinhämtning som avser datatrafik. Det är förbjudet att inhämta sådana uppgifter.

Underrättelseskyldigheten

G10-lagens 12 § innehåller bestämmelser om anmälningar till berörda parter. En person som varit föremål för en åtgärd ska ges en underrättelse om detta efter att åtgärden upphört. Ingen underrättelse görs dock, om underrättelsen äventyrar syftet med åtgärden eller om man kan förutspå en avsevärd olägenhet för förbundsrepublikens eller en delstats allmänna intresse. Om en underrättelse inte gjorts inom tolv månader från åtgärdens slut, ska den uteblivna anmälan överföras för behandling av G10-kommissionen, som förordnar att en förlängning av tiden för uppskovet.

Lagen innehåller inte bestämmelser om någon allmän skyldighet för en underrättelsemyndighet att ge en underrättelse om att en person varit föremål för underrättelseinhämtning. I 15 § i BfV-lagen finns det bestämmelser om lämnande av uppgifter till en registrerad. På begäran av en registrerad kan en myndighet ge uppgifter om personuppgifter som gäller honom eller henne, om begäran är specificerad i den mån att den innehåller en hänvisning till ett konkret fall och personen har ett särskilt intresse att få uppgift som berör honom eller henne. Enligt 2 mom. i paragrafen är det möjligt att avstå från att ge uppgifter, om utlämnandet av uppgifterna äventyrar till exempel myndighetens skötsel av uppgifter.

5.2.4.5 Nederländerna

Allmänt

I Nederländerna innehas ansvaret för underrättelseverksamheten av den allmänna underrättelse- och säkerhetstjänsten Algemene Inlichtingen en Veiligheidsdienst, AIVD) och den militära underrättelse- och säkerhetstjänsten (Militaire Inlichtingen- en Veiligheidsdienst, MIVD). Tjänsternas verksamhet regleras i lagen om underrättelse- och säkerhetstjänster från år 2017 (Wet op de inlichtingen- en veiligheidsdienst, 2017, nedan Wiv-lagen). Lagen ersatte den tidigare Wiv-lagen från år 2002.

I Nederländerna har underrättelselagstiftningens funktion bedömts av en kommitté som år 2021 gav flera rekommendationer för att utveckla underrättelselagstiftningen. En temporär lag (Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen) trädde i kraft i juli 2024 och den ger myndigheterna möjlighet till effektivare verksamhet i den förändrade säkerhetsmiljön och i synnerhet mot statliga cyberhot. Den temporära lagen gäller till och med den 1 juli 2028.

Med avvikelse från Wiv-lagen ger lagen möjlighet exempelvis till att lagra ospecificerat datamaterial (bulk dataset) längre än de 18 månader som föreskriv i Wiv-lagen. Enligt artikel 27.1 i Wiv-lagen ska behovet av ospecificerat datamaterial bedömas så fort som möjligt och senast inom 18 månader. Obehövlig data ska utplånas i samband med denna bedömning. I enlighet med artikel 14b och 14ba i den temporära lagen är det möjligt att genom ett ministerbeslut förlänga förvaringen av icke-granskat ospecificerat datamaterial. Ett beslut om förlängning av lagringen kan göras för ett år åt gången och den totala maximitiden har inte föreskrivits. I enlighet med punkt 3 i artikel 14 ba ska ett beslut om förlängningen aviseras till den kommission som övervakar underrättelseverksamheten (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten CTIVD).

Enligt artikel 25.1 i Wiv-lagen har underrättelsetjänsterna rätt att inhämta uppgifter bland annat ur allmänt tillgängliga källor. Underrättelseinhämtning som omfattas av de ordinarie befogenheter förutsätter inte något ministertillstånd och inte heller något godkännande av tillsynsnämnden (Toetsingscommissie Inzet Bevoegdheid, TIB). Inget ministertillstånd förutsätts heller för underrättelseinhämtning enligt artikel 39 i lagen från förvaltningsorgan, tjänstemän eller andra som kan anses kunna lämna behövliga uppgifter. Tillsynsnämnden är ett oberoende organ, som i förväg bedömer om befogenheterna för underrättelseinhämtning är lagenliga.

Med stöd av artikel 45.1 i Wiv-lagen har underrättelsetjänsterna, om de föreskrivna förutsättningarna är uppfyllda, rätt att göra intrång i ett automatiskt system antingen genom att använda tekniska hjälpmedel, falska signaler, falska nycklar, falsk identitet eller via ett automatiskt system tillhörande tredjepart. Utövning av denna befogenhet är tillståndspliktig. Enligt artikel 5 omfattar utnyttjande av ett system tillhörande tredjepart inte installation av tekniska anordningar.

Underrättelseskyldigheten

Enligt artikel 59 i Wiv-lagen ska myndigheterna fem år efter vissa åtgärders slut och därefter årligen bedöma om det är möjligt att ge en underrättelse om en åtgärd till den person som varit föremål för den. De åtgärder som nämns i artikeln täcker öppnande av brev, riktad bevakning av kommunikation och besök i en bostad. Det är dock möjligt att låta bli att ge en underrättelse utifrån flera grunder, bland annat för att skydda verksamhet eller för att inte äventyra den nationella säkerheten. I situationer där en underrättelse inte kan ges eller om det i praktiken är omöjligt att ge den, ska en anmälan göras till tillsynskommissionen med en motivering om varför en underrättelse inte har kunnat ges till den berörda parten.

5.2.4.6 Cyberåtgärder på det internationella planet

Internationellt ingripande i funktionen för informationssystem som hotar landets försvar och den nationella försvaret har i typfallet varit verksamhet om vilken det inte egentligen alls funnits information i de offentliga källorna. Under de senaste åren har detta dock ändrats. Vissa länder

har offentligt framhållit möjligheten att ingripa i funktionen för informationssystem som hotar landsförsvaret eller den nationella säkerheten.

I fråga om lagstiftningens precision varierar dock situationen. Vissa länder har utfärdat bestämmelser om en möjlighet för myndigheten med ansvar för underrättelseinhämtning utomlands att utöver underrättelseinhämtning vidta även andra behövliga åtgärder för att skydda landsförsvaret och den nationella säkerheten. Bland dessa stater har Förenade kungariket i sin nationella cybersäkerhetsstrategi offentligt belyst möjligheten till aktiva cyberåtgärder, med fokus även på åtgärdernas laglighetsgrund. I och med att lagstiftningen är jämförelsevis diffus, vidtas åtgärderna ofta som ett samarbete mellan flera myndigheter genom att förena deras befogenheter. I Förenade kungarikets åtgärder deltar åtminstone signalspaningsmyndigheten GCHQ och utrikes underrättelsetjänsten SIS. Vidtagandet av cyberåtgärder baserar sig på tre lagar: 1) Intelligence Services Act 1994 (ISA), 2) the Investigatory Powers Act 2016 (IPA) och 3) the Regulation of Investigatory Powers Act 2000 (RIPA). Bland de myndigheter som fastställts i lagarna har SIS i lagen föreskrivits en rättighet att utöver inhämtande av information även vidta åtgärder utomlands.

Kanada företräder en annan syn. I den kanadensiska lagen om kommunikationssäkerhetsverket (Communications Security Establishment Act) har verket tilldelats en möjlighet att vidta aktiva cyberåtgärder. Enligt artikel 19 i lagen har verket mandat att vidta aktiva cyberåtgärder via den globala datainfrastrukturen eller med hjälp av den för att försvaga, störa, påverka, besvara eller ingripa i intentioner eller verksamhet av en utländsk person, stat, organisation eller terroristgrupp till den del som de anknyter till de internationella relationerna, försvaret eller säkerheten.

På våren 2025 godkände det japanska parlamentet en lag, med stöd av vilken de japanska myndigheterna kan vidta aktiva cyberåtgärder. Lagen ger polisen och själförsvarstrupperna möjligheter att avvärja cyberhot även i förväg och i samarbete med allierade.

År 2026 bereds en reform av lagstiftningen om utlandsunderrättelsetjänsten i Tyskland och i och med den får underrättelsetjänsten ännu mer omfattande befogenheter även till aktiva åtgärder. I lagpropositionen föreslås att den tyska utlandsunderrättelsetjänsten får rätt att till aktiva åtgärder, såsom förlamning av sabotageprogram och servrar, utomlands om det handlar om ett hot mot den nationella säkerheten. Befogenheterna i lagförslaget täcker även åtgärderna annanstans än i cybermiljön, såsom sabotageattacker.

Även om det inte i någon omfattande grad är känt i vilken grad de olika staterna vidtar aktiva cyberåtgärder, är det möjligt att utifrån ovan beskrivna exempel bedöma att allt fler stater strävar efter att avvärja cyberhot även utanför den egna statens gränser. Även i fallen i ovan beskrivna exempel betonas de randvillkor som den internationella rätten ställer för verksamheten och verksamheten är kraftigt övervakad.

6 Remissvar

6.1 Utlåtandena om arbetsgruppens betänkande

Utkastet till regeringens proposition var på remiss i tjänsten Utlåtande.fi mellan den 28 november 2025 och den 16 januari 2026.

Ett utlåtande begärdes av följande aktörer: ministerierna, Underofficersförbundet, Amnesty International, Finländska sektionen, Riksdagens justitieombudsmans kansli, Electronic Frontier Finland - Effi ry, Finlands näringsliv, FiCom ry, Finnish Information Security Cluster (FISC)

Kyberala ry, Helsingfors hovrätt, Helsingfors tingsrätt, Förhandlingsorganisationen för offentliga sektorns utbildade FOSU rf, Högsta domstolen, Justitiekanslersämbetet, Polisstyrelsen, Huvudstaben, Befälsförbundet, Reservistförbundet, Gränsbevakningsväsendet, Skyddspolisen, Suomen Erillisverkot Oy, Finlands Reservofficersförbund ry, Teknologiateollisuus ry, Underrättelsetillsynsombudsmannen, Dataombudsmannens byrå, Republikens presidents kansli, Trafik- och kommunikationsverket Traficom, Tullen, Upseeriliitto ry, Bevärförbundet rf, Skatteförvaltningen, Riksåklagarens byrå.

Utlåtanden mottogs från 41 aktörer. Ett utlåtande gavs av Underofficersförbundet rf, Riksdagens justitieombudsmans kansli, Electronic Frontier Finland - Effi ry, Finlands Näringsliv EK, Pensionsskyddscentralen, FiCom ry, Finnish Information Security Cluster (FISC) - Kyberala ry, Helsingfors hovrätt, Helsingfors tingsrätt, Keva, Kommunikationsministeriet, Miesten hypogonadikuntoutujien järjestö ry, Justitiekanslersämbetet, Justitieministeriet, Polisstyrelsen, Puolustus- ja Ilmailuteollisuus PIA ry, Huvudstaben, Befälsförbundet, Reservistförbundet, Gränsbevakningsväsendet, Inrikesministeriet, Skyddspolisen, Suomen Erillisverkot Oy, Finlands Reservofficersförbund ry, Åklagarmyndigheten, Teknologiateollisuus ry, Underrättelsetillsynsombudsmannen, Dataombudsmannens byrå, Republikens presidents kansli, Traficom, arbets- och näringsministeriet, utrikesministeriet, Upseeriliitto ry, statsrådets kansli, finansministeriet, Bevärförbundet rf, Skatteförvaltningen, Riksåklagarens byrå och miljöministeriet. Dessutom gavs ett utlåtande av två enskilda personer.

Dessutom finns utlåtandena om utkastet och det övriga beredningsunderlaget för projektet för påseende på statsrådets webbplats under beteckningen PLM007:00/2024. .

I utlåtandena ansågs det vara viktigt att säkerhetsmyndigheterna i den nuvarande säkerhetsmiljön har tillräckliga möjligheter att förfara, med hänsyn till den tilltagande tekniska utvecklingen.

I det utkast till regeringsproposition som var på remiss föreslogs en möjlighet för försvarsgrenarna att delta ännu mer självständigt i militär underrättelseverksamhet. Dessutom föreslogs ordinarie användning av informationskällor för försvarsgrenarna. I utlåtandena tog man ställning till att underrättelseverksamhet i enlighet med motiveringarna till nuvarande 10 § i grundlagen har tilldelats som en uppgift endast för skyddspolisen och huvudstaben och Försvarsmaktens underrättelsetjänst, vilka verkar som militärunderrättelsemyndigheter. Eftersom den ändring som föreslogs i det utkast som var på remiss ledde till missförstånd i fråga om försvarsgrenarnas självständighet i underrättelseverksamheten, slopades förslaget till en egen paragraf för försvarsgrenarna vid den fortsatta beredningen och de behövliga ändringarna gjordes genom ändringar av den gällande bestämmelsen.

På motsvarande sätt riktade remissinstanserna uppmärksamhet på deltagandet i militär underrättelseverksamhet av personer som avgått från en militärunderrättelsemyndighet och i praktiken uppnått Försvarsmaktens pensionsålder. Eftersom pensionsåldern stigit hos Försvarsmakten, den övre åldersgränsen för reserven höjts och det även är möjligt att göra andra tjänstearrangemang, visade sig den föreslagna bestämmelsen vara onödig.

Förslaget till bestämmelse om ändringar i regleringen kring samarbete med andra myndigheter och med företag och andra sammanslutningar ansågs vara befogade och behövliga.

I fråga om 18 a § i lagförslag 1 i propositionen (samverkan med Gränsbevakningsväsendet) anmärktes att det enligt motiveringarna till 10 § i grundlagen och grundlagsutskottets ståndpunkter inte är möjligt att tilldela en ställning som underrättelsemyndigheter för andra än

skyddspolisen, huvudstaben och Försvarsmaktens underrättelsetjänst. Dessutom riktades uppmärksamhet på att Gränsbevakningsväsendets roll att stödja militärunderrättelsemyndigheten kan fördunkla Gränsbevakningsväsendets myndighetsroll. Uppmärksamhet riktades även på att vidtagandet av åtgärderna i gränsbevakningslagen med koppling Schengenområdets gränskodex delvis eller helt i underrättelsesyfte kan vara problematiskt med tanke på principen om ändamålsbundenheten och iakttagandet av Schengenområdets gränskodex.

Vid den fortsatta beredningen har man strävat efter att förtydliga bestämmelsen och förbättra motiveringarna.

I fråga om 20 § i lagförslag 1 i utkastet (internationellt samarbete) riktade remissinstanserna uppmärksamhet på att utbudet av metoder för en utländsk tjänsteman utvidgas i och med den föreslagna ändringen till att täcka även metoder som innebär en inskränkning av skyddet för hemligheten i fråga om meddelanden. Detta kan anses vara en utvidgning i förhållande till vad som konstateras i motiveringarna till den gällande lagen.

Vid den fortsatta beredningen har man stävat efter att utveckla motiveringarna. I varje fall verkar en utländsk tjänsteman så som för närvarande under styrning och övervakning av militärunderrättelsemyndigheten och den ansvarar för de tillstånd och beslut som åtgärderna förutsätter.

I fråga om 33 § (beslut om teknisk observation av utrustning) i lagförslag 1 riktade remissinstanserna uppmärksamhet på att vid teknisk observation av utrustning som hänför sig till en person kan domstolen inte kontrollera till vilka alla anordningar och programvaror befogenheten sist och slutligen hänför sig. Å andra sidan kan teleavlyssning redan för närvarande riktas på personbasis. Helsingfors tingsrätt konstaterade vidare att ändringen inte väsentligt påverkar rättsskyddet för målpersonen, eftersom förutsättningarna för användning av en metod för underrättelseinhämtning vanligen bedöms i förhållande till dess objekt och inte till en viss enskild anordning.

Redan för närvarande fattas ett beslut om att foga en ny teleterminalutrustning eller teleadress till ett tillstånd vid till exempel teleavlyssning som gäller en person av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Beslutet fattas alltid under tjänsteansvar. Nya teleterminalutrustningarna och teleadresser ska fogas till ett nytt domstolsyrkande som gäller samma objekt.

Vid den fortsatta beredningen beslutade man att lyfta ovan beskrivna förfarande till lagnivå. I motiveringarna har man dessutom betonat att underrättelsetillsynsombudsmannens övervakning i fråga om användning av personbaserade metoder för underrättelseinhämtning gäller även för nya teleterminalutrustningar, teleadresser, anordningar och programvaror som fogats till befogenheten. På motsvarande sätt ska en militärunderrättelsemyndighet underrätta underrättelsetillsynsombudsmannen om ett beslut om foga ny utrustning till beslutet i samma förfarande som då myndigheten fattar ett beslut om användningen av metoden för underrättelseinhämtning.

I fråga om 42 § i lagförslag 1 i utkastet (installation och avinstallation av anordningar, metoder eller programvara) riktades uppmärksamhet på i hur omfattande grad åtgärder vidtas, om verksamheten ska anmälas och hur företag och sammanslutningar som förfar lagligt kan minska sina risker i anknytning till förtroendet. Dessutom uttrycktes en oro för att nivån på cybersäkerheten i ett företag eller en sammanslutning som förfar lagligt i Finland kan försvagas.

De åtgärder som avses i bestämmelsen handlar om sådana åtgärder som en militärunderrättelsemyndighet kan vidta redan för närvarande med stöd av lagen och även omfattningen är den samma. Således kan det inte anses vara sannolikt att nivån av cybersäkerheten inte heller framöver försvagas. Med tanke på militärunderrättelsemyndigheternas uppgifter är det även centralt att de behövliga instanserna ges information om till exempel observerade sårbarheter. Anordningarna, metoderna och programvarorna övervakas kontinuerligt av militärunderrättelsemyndigheten och andra instanser får inte möjlighet att använda dessa. Detta gäller även för sårbarheter som militärunderrättelsemyndigheten själv genomfört. Dessutom innehåller bestämmelsen även separata bestämmelser om till exempel avinstallation av en programvara.

I utlåtandena riktades även uppmärksamhet på att åtgärder kan vidtas inom hemfridsskyddet. Detta är dock inte möjligt eftersom paragrafens 1 mom. på samma sätt som annanstans i lagen uttryckligen förbjuder att en militärunderrättelsemyndighet vidtar åtgärder och utövar befogenheter i ett hemfridsskyddat utrymme.

I utlåtandena påpekades att verksamheten handlar om utövande av betydande offentlig makt. Så som lagts fram i regeringens proposition i avsnittet om lagstiftningsordningen, anses att det inte handlar om avsevärd utövning av offentlig makt, eftersom verksamheten inte är förenad med självständigt beslutsfattande och åtgärderna sker inom ramen för myndighetens befogenhet.

I fråga om 46 a och 46 b § i lagförslag 1 i utkastet (täckoperation som genomförs uteslutande i datanät och beslut om sådan) riktades uppmärksamhet på att ändringen eller dess behov inte har motiverat i regeringspropositionen. Vid den fortsatta beredningen belystes de föreslagna ändringarna.

I utlåtandena riktades uppmärksamhet på hur befogenheten riktas och att den verkar vara mer vag än i den gällande lagen. I den version som var på remiss strävade man efter att den kan riktas mot ett hot som omfattas av befogenheten för militär underrättelseinhämtning, men vid den fortsatta beredningen beslöt man sig för en lösning där den riktas utifrån avgränsningen av personkretsen på samma sätt som föreskrivits för vissa andra metoder för underrättelseinhämtning.

I fråga om 61 a § i lagförslag 1 i utkastet (underrättelseinhämtning i hemlandet som avser statliga aktörers datasystem) riktades uppmärksamhet på befogenhetens omfattning och på hur den riktas samt definieringen av ett datasystem i tillståndsbehandlingen. Motiveringarna till bestämmelserna har preciserats och man har belyst att militärunderrättelsemyndigheten ofta känner till en väldigt exakt utgångssituation innan man börjar utöva en befogenhet.

Vid den fortsatta beredningen har man strävat efter att betona att föremålet för en metod för underrättelseinhämtning inte är till exempel en hel serversal, utan att militärunderrättelsemyndigheten med relativt stor precision kan rikta metoden mot en viss anordning som en statlig aktör använder i Finland. Således är föremålet för en metod för underrättelseinhämtning till en början en viss anordning och genom att bevaka dess verksamhet och uppgifter är det möjligt att närmare komma åt andra anordningar i informationssystemet. Det är dock möjligt att även andra personers kommunikation omfattas av inhämtandet av information, men denna information omfattas av direktutplåningsskyldigheten.

Vid den fortsatta beredningen har man till paragrafen fogat en bestämmelse som reglerar förfarandet i en situation där en ny anordning eller del av ett datasystem fogas som föremål för användning av metod för underrättelseinhämtning. Dessutom föreslås att bestämmelser utfärdas

om avbrytande av underrättelseinhämtning som avser datatrafik i Finland även i paragrafen om avbrytande av användning av en metod för underrättelseinhämtning.

I enlighet med principen om ändamålsbundenhet är det möjligt att genom befogenheten ingripa endast i en statlig aktörs kommunikation. Eftersom det handlar om en statlig aktörs informationssystem kan det inte anses vara sannolikt att slumpmässiga utomstående personer använder datasystemet för sin privata kommunikation. Således kan kommunikationen i utgångspunkten anses vara statlig kommunikation. Om även annan kommunikation förekommer i datasystemet, omfattas den av direktutplåningsregleringen.

I utlåtandena riktades uppmärksamhet på att bestämmelsen inte entydigt gäller endast för delar av informationssystem i Finland. Vid den fortsatta beredningen riktades uppmärksamhet på detta.

I utlåtandena förde man även fram att befogenheten till och med kan förbättra rättsskyddet i det hänseendet att den domstol som beslutar om ett tillstånd till underrättelseinhämtning som avser datasystem kan ha bättre möjligheter att bedöma den helhet som utgörs av metoden för underrättelseinhämtning.

I fråga om 62 a och 62 b § i lagförslag 1 i utkastet (förhindrande av användningen av datasystem eller störande av dess funktion för avvärjande av allvarlig fara) uttrycktes i utlåtandena en oro för att åtgärderna kan orsaka en eskalering och försämra Finlands utrikes- och säkerhetspolitiska ställning. Detta ansågs förutsätta utrikes- och säkerhetspolitiskt beslutsfattande och tväradministrativ beredning. Det finns skäl att ovan konstaterade omständigheter framgår även av själva paragrafen. Vid den fortsatta beredningen konstaterade man att observationerna var befogade.

I utlåtandena uppmärksammades även att bestämmelsens förhållande till egentlig underrättelseinhämtning förblir oklar på bestämmelsenivå. Vid den fortsatta beredningen beslöt man sig för att foga regleringen till en del av 62 § i lagen.

Beslutsfattandet om vidtagandet av åtgärder orsakade oklarhet bland remissinstanserna. Det utkast som var på remiss kunde ge en bild av att huvudstabens underrättelsechef kan fatta beslut om dessa åtgärder på egen hand. Detta har dock inte varit avsikten. Vid den fortsatta beredningen har detta förtydligats på bestämmelsenivån och i motiveringarna.

I en del av utlåtandena ansågs målen med den föreslagna regleringen vara värda att understödja.

I fråga om 66 § i lagförslag 1 i utkastet (behandling av tekniska data för identifiering av en del av ett kommunikationsnät och för identifiering av dirigeringen av och ändringar i datatrafiken) riktades uppmärksamhet på hur mängden uppgifter som lagras bedöms och hur omfattande lagringen är.

Vid den fortsatta beredningen har man strävat efter att förtydliga motiveringarna. Fem procent av kapaciteten i en del av ett kommunikationsnät baserar sig på den tekniska maximikapaciteten i en enskild fiber, vilket förblir standard. Det system i vilket informationen lagras ska genomföras på så sätt att det i systemet är möjligt att lagra endast fem procent denna maximikapacitet per sekund. Därefter förblir den lagrade informationen i 18 månader i systemet, varefter den utplånas.

En del av ett kommunikationsnät som överskrider Finlands gräns, inte Finlands kommunikationsnät i sin helhet, har alltid fastställts som mål för befogenheten. Kapaciteten i

en del av kommunikationsnätet kan i praktiken inte ändras på ett obemärkt sätt, eftersom tekniska ändringar syns till exempel som avbrott i datatrafiken i en del av kommunikationsnätet. Det kan förmodas att kapaciteten i en del av kommunikationsnätet ökar i och med eventuella tekniska ändringar, varvid systemets attribut förblir oförändrade och information lagras i en mängd som motsvarar den tidigare kapaciteten. En mer omfattande kvantitativ lagring förutsätter systemändringar.

I utlåtandena belystes uppfattningen om att kan en militärunderrättelsemyndighet med stöd av bestämmelsen kan extrahera enskilda uppgifter från de lagrade uppgifter och utreda uppgiftskällan till exempel med stöd av 104 § i lagen. Detta är dock inte möjligt eftersom lagrade uppgifter kan behandlas i de föreslagna separata fallen som regleras i lagen, det vill säga under de förutsättningar föreskrivs i 67 a § samt i 68 och 70 §. Ett domstolstillstånd är alltid en förutsättning för att använda uppgifter. I sista hand kan en person som anknyter till en enskild uppgift utredas endast genom att använda underrättelseinhämtning som avser datatrafik, vilket förutsätter användning av sökbegrepp.

I utlåtandena riktades uppmärksamhet på att förbudet att bilda en analys som redogör för en enskild person inte ska slopas. Vid den fortsatta beredningen har det uttryckliga förbudet återställts.

I utlåtandena om 67 a § i lagförslag 1 i utkastet (underrättelseinhämtning som avser datatrafik för fastställande av sökbegrepp) ansågs hänvisningen till regelbundenhet i datatrafiken i bestämmelsen vara oklar. Vid den fortsatta beredningen beslutade man sig för att slopa slumpmässigheten.

I utlåtandena påpekade man att befogenheten inte får möjliggöra att man kringgår egentligt underrättelseinhämtning som avser datatrafik. Vid den fortsatta beredningen har bestämmelsen preciserats och i bestämmelsen har man infört uttryckliga begränsningar som gäller till exempel att användningen av befogenheten inte får leda till att man får information som beskriver en persons privatliv eller kommunikationens innehåll.

I utlåtandena riktades uppmärksamhet på att datatrafikens slumpmässigheten kan anses lämna utrymme för tolkning. Vid den fortsatta beredningen beslöt man sig för att avlägsna detta, eftersom slumpmässig datatrafik i varje fall rör sig i en del av kommunikationsnätet, det vill säga att det inte är möjligt att helt exakt i förväg veta vilken aktörs datatrafik som rör sig i en del av kommunikationsnätet vid respektive tidpunkt. En annan sak som i praktiken styr mot slumpmässigheten är att föremålet för befogenheten kan vara fem procent av datatrafiken i en del av kommunikationsnätet.

I fråga om 68 och 70 § i lagförslag 1 i utkastet tog man ställning till att sökbegrepp som hänför sig till innehållet i ett meddelande inte begränsas i bestämmelserna. Vid den fortsatta beredningen har regleringen preciserats och användning av sökbegrepp som utgörs av ord och hänför sig till innehållet har bundit till användning av andra sökbegrepp. Andra än språkliga sökbegrepp (såsom tekniska data) kan användas i oförändrad form.

I utlåtandena riktades uppmärksamhet på att ändringen inte har bedömts i motiveringarna till lagstiftningsordningen. Vid den fortsatta bedömningen har bristen åtgärdats.

I fråga om 78 § i lagförslag 1 i propositionen (tryggande av informationskällor) lade man fram att förslaget innehåller begrepp som kan anses lämna utrymme för tolkning och vars innehåll ska förtydligas i motiveringarna. Vid den fortsatta beredningen har bestämmelsen och dess

motiveringar preciserats. Bland annat bistånd har ändrats till termen ordna, som används i 17 kap. i strafflagen.

I fråga om 89 § i lagförslag 1 i utkastet (underrättelse om användning av metod för underrättelseinhämtning) riktades uppmärksamhet på om underrättelsetillsynsombudsmannens övervakning och möjligheten att göra begäranden om undersökning och klagomål fyller rättsskyddsbristen. Vissa remissinstanser riktade uppmärksamhet på att man i stället för att reducera anmälningsskyldigheten ska stärka den eller åtminstone bibehålla den i oförändrad form. Å andra sidan konstaterades i utlåtandena att ärendet ska motiveras på ett mer övertygande sätt i motiveringarna. Vid den fortsatta beredningen har motiveringarna preciserats.

I fråga om 96 § i lagförslag 1 i utkastet (biståndsskyldighet för kommunikationsförmedlare och leverantörer av datacentraltjänster) lade man fram att den föreslagna ändringen kan leda till en situation där företagen och sammanslutningar måste avstå från ända till ända-kryptering. Vid den fortsatta beredningen konstaterade man att ingen sådan reglering föreslås. Detta fördes dock fram i motiveringarna.

I utlåtandena påpekades att regleringen kring ersättningar som betalas till företag för bistånd ska utvecklas på så sätt att en ersättning betalas för allt bistånd i en omfattning som motsvarar vad som föreskrivits i fråga om genomförande av den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter. Vid den fortsatta beredningen konstaterades att det inte är möjligt att avgöra ärendet i detta samband, eftersom ärendet gäller en större grupp myndigheter än endast militärunderrättelsemyndigheter. Till exempel i fråga om teleavlyssning används teleavlyssningssystemet avsevärt mer i brottsbekämpningen än i underrättelseverksamhet. Således är det inte ändamålsenligt att ändra sakläget i projektet för att ändra lagen om militär underrättelseverksamhet.

I utlåtandet påpekades att den utvidgade biståndsskyldighet som föreslagits i det utkast som var på remiss även var diffus och avsevärt utvidgar tillämpningen av bestämmelsen.

Vid den fortsatta beredningen konstaterades tillämpningsområdet vara för brett och i propositionen gäller biståndsskyldigheten endast för leverantören av datacentraltjänster på det sätt som den definierats i cybersäkerhetslagen. Dessutom har termen telenät ändrats till kommunikationsnät i propositionen, vilket kan anses beskriva nätet bättre även med tanke på lagen om tjänster inom elektronisk kommunikation.

I fråga om 99 § i lagförslag 1 i utkastet (ersättningar till kommunikationsförmedlare och leverantörer av informationssamhällets tjänster) påpekades att regleringen kring ersättningar som betalas till företag för bistånd ska utvecklas på så sätt att en ersättning betalas för allt bistånd i en omfattning som motsvarar vad som föreskrivits i fråga om genomförande av den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter.

Vid den fortsatta beredningen konstaterades att det inte är möjligt att avgöra ärendet i detta samband, eftersom ärendet gäller en större grupp myndigheter än endast militärunderrättelsemyndigheter. Till exempel i fråga om teleavlyssning används teleavlyssningssystemet avsevärt mer i brottsbekämpningen än i underrättelseverksamhet. Således är det inte motiverat att ändra sakläget i projektet för att ändra lagen om militär underrättelseverksamhet.

I fråga om 104 § i lagförslag 1 i utkastet (rätt att få information av privata sammanslutningar) ansågs den föreslagna ändringen vara befogad i utlåtandena. I utlåtandena framlades dock en uppfattning om att man genom att förslaget försöker kringgå till exempel teleavlyssning.

Förslaget gäller dock enskilda uppgifter och ger inte kommunikationsförmedlarna omfattande skyldigheter att till exempel behandla uppgifter för en myndighets räkning. Dessutom motsvarar regleringen vad som föreskrivits i 4 kap. 3 § i polislagen.

På samma sätt som lagts fram tidigare har en leverantör av samhällets tjänster ersatts med leverantör av datacentraltjänster vid den fortsatta beredningen.

I utlåtandena om 8 b § i lagförslag 2 i utkastet (inhämtande av information från allmänt tillgängliga källor) riktades uppmärksamhet på att möjligheten att använda påhittade, vilseledande eller förtäckta uppgifter i allmänt tillgängliga lagliga tjänster inte får leda till att myndigheten inte betalar för tjänsten eller i övrigt orsakar skada för tjänsteleverantören. Å andra sidan förde man i utlåtandena fram att det är ändamålsenligt att utsträcka skyddet till och med längre än så, såsom att betala avgiften under täckmantel.

I utlåtandena riktade man även uppmärksamhet på regleringen till den del hur regleringen kring enskilda myndigheter förhåller till regleringen för andra myndigheter på rättsordningsnivå.

Vid den fortsatta beredningen har man fört fram de nämnda omständigheterna. Den bild som eventuellt ges utlåtandena, enligt vilken myndigheterna strävar efter att använda kommersiella tjänster utan att betala, kan i varje fall anses vara obefogad.

I fråga om 36 a § i lagförslag 2 i utkastet (ledigförklarande av en tjänst) påpekades att man i propositionen mer ingående ska beakta den motsvarande regleringen till exempel i fråga om tillsättning av skyddspolisens tjänster. Dessutom gjordes en hänvisning till grundlagsutskottets utlåtande (GrUU 45/2022 rd). Vid den fortsatta beredningen har omständigheter som gäller nödvändighetsbedömningen förts fram noggrannare i bestämmelsen och i dess motiveringar.

Den ändring av strafflagen som föreslogs i utkastet slopades som en obehövlig ändring, eftersom tillräcklig reglering kan genomföras genom att ändra endast lagen om militär underrättelseverksamhet.

I utlåtandena riktade man uppmärksamhet på de ändringsförslag som gäller tillgången på uppgifter, i fråga om vilka man konstaterade att största delen av de uppgifter som ändringarna gäller är tillgängliga redan med stöd av den gällande lagen. Dessutom preciserades de andra anknutna lagarna i utkastet och motiveringarna till dessa.

I fråga om behandlingen av personuppgifterna riktade man i utlåtandena uppmärksamhet på om man annanstans i lagen för Försvarsmakten föreskrivit en rätt att utan hinder av sekretessbestämmelserna lämna ut personuppgifter ur ett eget personregister genom en teknisk förbindelse eller som dataset som en rätt som är överensstämmande med militärunderrättelsemyndigheternas rätt att få information. Det förblir oklart vad som avses med jämförelse av uppgifter. Vid den fortsatta beredningen har man strävat efter att förtydliga detta. I varje fall motsvarar regleringen vad som föreskrivits för skyddspolisen.

I utlåtandena riktade man därtill uppmärksamhet på att man i fråga om behandlingen av personuppgifter i det utkast som var på remiss inte egentligen alls behandlade ärendet i motiveringarna till lagstiftningsordningen och att grundlagsutskottets nyare utlåtandepraxis i ärendet inte beaktades.

Vid den fortsatta beredningen har man strävat efter att beakta ovan beskrivna anmärkningar. Vid den fortsatta beredningen förde man dessutom fram behovet av att utveckla regleringen

kring trygghet av en tjänsteman inom underrättelseinhämtning och akuta beslut om teleavlyssning.

6.2 Utlåtandet av bedömningsrådet för lagstiftningen

Bedömningsrådet för lagstiftningen gav ett utlåtande om utkastet till propositionen den 4 maj 2026 (ärendenummer VN/13863/2025-VNK-3). Bedömningsrådet ansåg att utkastet till regeringsproposition iakttar anvisningen om konsekvensbedömning vid lagberedning på tillfredsställande sätt. Bedömningsrådet rekommenderar att utkastet till proposition korrigeras i enlighet med rådets utlåtanden innan regeringens proposition överlämnas.

Utkastet till proposition ger i huvudsak en uppfattning om bakgrunden till ärendet, målen och de centrala förslagen. I utkastet till proposition har konsekvenserna behandlats ur flera synvinklar, men de centrala slutsatserna av konsekvensbedömningen och konsekvenskedjorna framgår inte till alla delar på ett tydligt sätt. De centrala utvecklingsobjekten gäller i synnerhet en mer utförlig beskrivning av konsekvensernas omfattning, inriktning och osäkerhet samt att konsekvensbedömningen på flera punkter är av mer allmän nivå än bedömningen av nuläget.

Bedömningsrådet anser att konsekvenserna behandlats i relativt bred omfattning i utkastet till proposition och att utkastet täcker de centrala konsekvensområdena. Rådet anser även att det är förtjänstfullt att konsekvensavsnittet inte begränsar sig endast till att beskriva de eftersträlvade nyttorna, utan att man i utkastet på flera punkter identifierar även ingrepp i rättigheterna, tekniska risker, olägenheter som hänför sig till företagsverksamhet samt spänningar i de internationella relationerna.

Bedömningsrådet anser att då bedömningen av nuläget är detaljerad och tydlig, lämnar konsekvensbedömningen på flera punkter på en mer allmän nivå – tyngdpunkten i bedömningarna övergår ofta till beskrivningarna av ändringarna och motiveringarna.

Bedömningsrådet anser att avsnittet om företagskonsekvenserna av utkastet till proposition identifierar flera väsentliga konsekvensmekanismer. Bedömningen hänför sig bland annat till administrativa kostnader, biståndsskyldigheterna, behandlingen av dataskyddsincidenter, förtroendet, den immateriella egendomen och cyberrisker. Bedömningen förblir dock till stor del kvalitativ och inga kvantitativa uppskattningar läggs fram om konsekvensernas omfattning. I utkastet till proposition har man även identifierat eventuella nyttor före företagen, men bedömningen av nyttokonsekvenserna förblir dock allmän.

Bedömningsrådet riktar uppmärksamhet på att utkastet till propositionen inte innehåller något separat avsnitt om konsekvenserna för den offentliga ekonomin. Enligt anvisningen om konsekvensbedömningar ska de ekonomiska konsekvenserna struktureras som konsekvenser för de privata hushållen, företagen och den offentliga ekonomin.

Bedömningsrådet anser att avsnittet om konsekvenserna för samhällsekonomin och näringslivet i utkastet till proposition har motiverats utgående från att lagstiftningen om militär underrättelseverksamhet kan ha även positiva konsekvenser för företagen och samhällsekonomin. I utkastet till propositionen vore det dock nyttigt att mer utförligt än för närvarande beskriva med vilka slags konsekvensmekanismer sådana nyttor kan förmedlas till näringslivet och samhällsekonomin, hur betydande man finner dessa och på vad sådana uppskattningar baserar sig.

Bedömningsrådet anser att det är positivt att man i utkastet till proposition i omfattande grad identifierar kopplingarna till de grundläggande fri- och rättigheterna och de mänskliga

rättigheterna. Utkastet till proposition identifierar frågor med koppling till skyddet för privatlivet, skyddet för ett förtroligt meddelande, rättsskyddet och skyddet för personuppgifter. Dessutom innehåller utkastet ett omfattande separat avsnitt om förhållandet till grundlagen och lagstiftningsordningen.

Bedömningsrådet anser att sättet att presentera den helhet som gäller de grundläggande fri- och rättigheterna och de mänskliga rättigheterna försämrats av upprepningar och ställvis långa meningar. I konsekvensbedömningen och i det senare avsnittet om grundlagen och lagstiftningsordningen behandlas delvis samma uppskattningar och motiveringar med lite olika ordalydelser, varför helheten blir tung.

Bedömningsrådet anser att myndighetskonsekvenserna har identifierats relativt väl i utkastet till proposition. Förslagen gäller bland annat militärunderrättelsemyndighetens befogenheter, Gränsbevakningsväsendets biståndsroll, informationsutbytet mellan olika myndigheter samt nya uppgifter och införandet av tekniska lösningar. Konsekvensbedömningen skulle dock förbättras av en närmare indelning av konsekvenserna enligt myndighetsaktör. I utkastet till proposition är det motiverat att mer utförligt än för närvarande specificera konsekvenserna för arbetsmängden, kompetensen, systemen och samordningen för åtminstone Försvarsmakten, Gränsbevakningsväsendet, underrättelsetillsynsmyndigheten, domstolarna samt de myndigheter som lämnar ut uppgifter.

Bedömningsrådet anser att det är positivt att utkastet till proposition identifierar konsekvenserna för informationshanteringen som ett separat konsekvensområde.

Bedömningsrådet anser att flera konsekvenser som gäller genomförandet och resursallokeringen till myndigheterna bedöms på relativt allmänt sätt i utkastet till proposition.

Bedömningsrådet anser att den centrala konsekvens som eftersträvas med propositionen gäller förstärkt försvar av landet och nationell säkerhet. Bedömningen av dessa konsekvenser stannar på en relativt allmän nivå, i synnerhet med beaktande av hur omsorgsfullt behovet av de föreslagna ändringarna har motiverats i beskrivningen av nuläget. Uppskattningen ger en uppfattning om konsekvensernas riktning, men redogör inte till alla delar tillräckligt tydligt för vilken extra nytta man enligt bedömning uppnår med de enskilda ändringarna jämfört med nuläget, hur ofta bristerna i nuläget i praktiken framträder eller på vad bedömningen av de olika säkerhetsnyttorna baserar sig. Bedömningsrådet anser dock att det är begripligt att alla konsekvenser på grund av deras natur inte till alla delar kan beskrivas exakt.

Bedömningsrådet anser att man i utkastet till proposition kvalitetsmässigt för fram regleringens eventuella konsekvenser för dataskyddet och samhällets funktionssäkerhet. Nyttornas omfattning, villkoren för att de ska realiseras och eventuella anseenderisker förblir dock på en relativt allmän nivå. Det vore nyttigt att i konsekvensbedömningen närmare bedöma hur ofta man uppskattar att nya befogenheter används och i vilka slags situationer konsekvenserna kan vara avsevärda.

Bedömningsrådet anser att utkastet till proposition identifierar gränsöverskridande konsekvenser. I detta konsekvensslag vore det dock nyttigt att närmare strukturera konsekvensen för det internationella underrättelsesamarbetet, Finlands relationer med andra stater och de situationer där det inte är möjligt att samarbeta med målstaten. Konsekvenserna ska behandlas även med tanke på olika risker.

Utifrån bedömningsrådets utlåtande har propositionens konsekvensbedömning kompletterats och redigerats. Det är inte möjligt att till alla delar göra någon uppskattning av konsekvenserna

eller att ge någon närmare riktgivande uppskattning på grund av att uppgifterna inte är offentliga.

7 Specialmotivering

7.1 Lagen om militär underrättelseverksamhet

11 §. Militärunderrättelsemyndigheter. Paragrafens 2 mom. ändras. Vid utförandet av underrättelseuppdrag är försvarsgrenarna på ett sätt som motsvarar nuläget fortfarande underställda militärunderrättelsemyndighetens styrning och övervakning. I och med förslaget kan Armén, Marinen och Flygvapnet utöver radiosignalspaning enligt den gällande lagen förlita sig på ordinarie användning av informationskällor av grundformen för att utföra ett underrättelseuppdrag. Försvarsgrenarna kan styra personen att inhämta information. Observationerna och lämnandet av information baserar sig alltid på personernas frivillighet och uppgifterna ska ha en koppling till militärunderrättelsemyndighetens underrättelseuppdrag.

Genom ändringen möjliggörs att uppgifter kan tas emot av en militärunderrättelsemyndighet även då personerna, till exempel då de rör sig i närheten av en gräns eller utomlands, upptäcker verksamhet som enligt dem avviker från det normala. Befogenheten till användning av informationskällor av grundformen är relevant även för informationskällan. Eftersom en informationskälla har en vilja att på eget initiativ berätta om sin information om ärenden som gäller verksamheten, är det befogat att han eller hon kan närma sig myndigheten under en tidpunkt och vid en plats som passar honom eller henne.

I fråga om försvarsgrenarnas radiosignalspaning görs inga ändringar och försvarsgrenarnas underrättelseinhämtning föreskrivs fortfarande i lagens 60 §.

15 §. Samordning av underrättelseverksamheten. Paragrafens 1 mom. ändras på så sätt att republikens president ändras till republikens presidents kansli. De centrala högsta tjänstemännen är företrädare i sammansättningen och inte heller ursprungligen har avsikten varit att republikens president deltar i samordningen. Redan den gällande lagen har tolkats på så sätt att en företrädare för republikens presidents kansli deltar i mötena, varför texten i författningen uppdateras för att motsvara nuläget.

18 §. Samarbete med andra myndigheter och med företag och andra sammanslutningar. I paragrafens 1 mom. görs en teknisk ändring och i bestämmelsen stryks ordet "uppgifter" i den första meningen och momentets andra mening, som hänvisar till lagen om behandling av personuppgifter inom Försvarsmakten. Hänvisningen till lagen om behandling av personuppgifter inom Försvarsmakten finns redan i 2 § i lagen, varför hänvisningen i 18 § 1 mom. kan anses vara onödig.

I paragrafens 2 mom. görs en teknisk ändring som gäller sabotageprogram. I och med ändringen upphävs 74 § i lagen. I nuläget har bestämmelsen bundit inhämtandet av information till utvecklande av metoderna och systemen för underrättelseinhämtning, det vill säga att utlämnandet av uppgifter om sabotageprogram har bundits till ett behov av underrättelseinhämtning. Detta kan anses vara en onödig avgränsning, eftersom utlämnande av uppgifter om sabotageprogram ska ske med så låg tröskel som möjligt. Utlämnandet är fortfarande bundet till en militärunderrättelsemyndighets uppdrag.

I den senare delen av bestämmelsen är utlämnandet av uppgifter bundet till behov med avseende på försvaret av landet eller för att skydda den nationella säkerheten. Detta innebär att det genom

att lämna ut uppgifter är möjligt att förbättra Finlands försvar eller den nationella säkerheten och att utlämnandet av uppgifter ska ha en koppling till dessa intressen.

Cybermiljöns betydelse i samhället och via det i försvaret av landet och den nationella säkerheten har fortsatt att öka ytterligare. I och med den tekniska utvecklingen vidareutvecklar även de avancerade så kallade APT-aktörerna sina förfaringssätt. I synnerhet dessa aktörer ska kunna lämna ut uppgifter om sabotageprogram med så låg tröskel som möjligt till aktörer som är kritiska med tanke på samhällets funktion. Det bör även observeras att information om sabotageprogram i fråga om de grundläggande fri- och rättigheterna inte omfattas av området för förtroliga meddelanden.

Bestämmelsens hänvisning till utlämnande av uppgifter om det behövs för att försvara landet eller skydda den nationella säkerheten, innebär även situationer där en militärunderrättelsemyndighets åtgärd kan leda till en risk för försvaret av landet eller den nationella säkerheten. Till exempel i en situation där en militärunderrättelsemyndighets åtgärd orsakar eskalatoriska åtgärder av den aktör som utgör föremål, till exempel en cyberattack mot finländska teleoperatörer, är det ändamålsenligt att militärunderrättelsemyndigheten meddelar risken till de aktörer som ansvarar för den kommunikationsinfrastruktur som är kritisk för Finland. Det motsvarande kan bli aktuellt även i fråga om kritiska aktörer. Genom meddelandet säkerställs att de aktörer som ansvarar för den kritiska infrastrukturen genom egna åtgärder kan förbereda sig och inleda egna åtgärder för att förebygga den skadliga verksamheten.

Om en militärunderrättelsemyndighet använder en upptäckt sårbarhet i en anordning eller programvara eller installerar ett kryphål i ett system som utgör objekt, är det på motsvarande sätt ändamålsenligt att militärunderrättelsemyndigheten underrättar innehavaren av anordningen eller datasystemet om detta, om det är möjligt och om sårbarheten eller militärunderrättelsemyndighetens egen åtgärd kan orsaka en fara för försvaret av landet eller den nationella säkerheten.

I paragrafens 3 mom. görs ändringar i paragrafhänvisningarna på grund av revideringen av den så kallade brandväggsregleringen (lagen om ändring av lagen om militär underrättelseverksamhet 169/2026).

Inga ändringar görs i paragrafens 4 mom., som innehåller bestämmelser om befogenheten att utfärda förordning.

18 a §. Samverkan med Gränsbevakningsväsendet. Paragrafen är ny. Det föreslås att paragrafen innehåller bestämmelser om möjligheten för Gränsbevakningsväsendet att biträda militärunderrättelsemyndigheterna i genomförandet av underrättelseuppdrag genom att medverka i användningen av metoder för underrättelseinhämtning. På samverkan mellan en militärunderrättelsemyndighet och Gränsbevakningsväsendet tillämpas i princip 18 § i lagen om militär underrättelseverksamhet, men i den praktiska verksamheten, i synnerhet i enskilda fall som gäller användningen av metoder för underrättelseinhämtning, har man dock observerat att det finns större behov av stöd från Gränsbevakningsväsendet. Det handlar med andra ord om kortvarigt utförande av enskilda uppdrag eller åtgärder i anknytning till ett underrättelseuppdrag och dessa utförs alltid på begäran av militärunderrättelsemyndigheten och inom ramen för dess befogenhet. I vissa situationer kan begäran ha gjorts i förväg eller så kan den i situationer som kräver en snabb reaktion ske via jourarrangemang mellan myndigheterna.

Militärunderrättelsemyndighetens åtgärder ska alltid kunna försvaras i förhållande till underrättelseinhämtningens betydelse. Även en begäran om en enskild åtgärd till Gränsbevakningsväsendet ska således alltid bedömas i förhållande till det eftersträfvade målet.

Dimensioneringen av åtgärderna för att inhämta information påverkas till exempel av hur väsentlig betydelse en viss enskild åtgärd har för inhämtandet av uppgifter om ett hot och genom åtgärden är det därtill inte tillåtet att ingripa i någons rättigheter mer än vad som är nödvändigt för att uppnå syftet med underrättelseinhämtningen.

Det föreslås att paragrafens 1 mom. innehåller bestämmelser om att Gränsbevakningsväsendet, utöver vad som föreskrivs i 18 § i lagen, kan ge hjälp i användningen av de metoder för underrättelseinhämtning som räknas upp i paragrafen. Med en enskild åtgärd med anknytning till en metod för underrättelseinhämtning avses exempelvis en teknisk installationsåtgärd i anknytning till användning av en metod eller observation som tillfälligt riktas mot en person eller en grupp av personer. Förteckningen är uttömmande och gäller i första hand endast de metoder för underrättelseinhämtning som enligt lagen kan vara föremål för ett beslut av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Dessa metoder för underrättelseinhämtning är observation och systematisk observation, teknisk avlyssning, optisk övervakning, teknisk spårning, teknisk observation av utrustning, inhämtande av identifieringsuppgifter om en teleadress eller teleterminalutrustning, installation och avinstallation av en anordning och en metod eller en programvara samt platsspecifik underrättelseinhämtning och kopiering. Gränsbevakningsväsendet kan dock biträda vid teknisk avlyssning, optisk observation och teknisk spårning, teknisk observation av utrustning och platsspecifik underrättelseinhämtning och kopiering även då tillstånd till användning av metoden för underrättelseinhämtning har getts av en domstol. Med andra ord blir det aktuellt med en grupp av metoder för underrättelseinhämtning, vars användning och anknutna enskilda åtgärder främst motsvarar de hemliga metoder för underrättelseinhämtning som Gränsbevakningsväsendet använder i dess uppdrag och beträffande vilka det redan har motsvarande praktisk erfarenhet i fråga om utförandet av ett enskilt uppdrag eller en enskild åtgärd. Gränsbevakningsväsendets åtgärder handlar dock inte om underrättelseverksamhet, eftersom behandlingen och analysen av de uppgifter som fåtts genom åtgärden alltid sker vid militärunderrättelsemyndigheten. Verksamheten sker inom ramen för militärunderrättelsemyndighetens befogenhet och under dess styrning och övervakning.

Av de uppräknade befogenheterna kan teknisk avlyssning, teknisk observation av utrustning och kopiering hänföra sig till innehållet i ett meddelande. Efter åtgärden styrs eller överförs uppgifterna direkt till militärunderrättelsemyndigheten. I fråga om metoder för underrättelseinhämtning som hänför sig till innehållet i ett meddelande handlar det ofta om en situation där man vidtar en installationsåtgärd och uppgifterna styrs direkt till militärunderrättelsemyndigheten.

Teknisk observation av utrustning kan hänföra sig direkt till ett meddelande, men i praktiken handlar Gränsbevakningsväsendets lokala befogenhet ofta om kopiering av uppgifterna i en teknisk anordning, såsom en lagringsenhet, och att överlämna kopian till en militärunderrättelsemyndighet. Således är det inte möjligt att vid Gränsbevakningsväsendet sätta sig in i meddelandets innehåll, vilket inte heller är syftet med åtgärderna. Även i fråga om kopiering handlar det om en teknisk åtgärd.

Militärunderrättelsemyndigheten har dock oberoende av detta en skyldighet att ordna utbildning om särdragen i metoderna för underrättelseinhämtning för den personal vid Gränsbevakningsväsendet som utför uppdrag eller åtgärder. Militärunderrättelsemyndigheten ansvarar likaså för beslut om eller ett tillstånd till metoden för underrättelseinhämtning samt för underrättelseskyldigheten enligt 89 §.

Naturen av de åtgärder som vidtas av Gränsbevakningsväsendet varierar enligt metod för underrättelseinhämtning. I vissa situationer kan en nödvändig åtgärd handla om installation av

en anordning, metod eller programvara, medan till exempel teknisk avlyssning även kan förutsätta att föremålet bevakas från ett visst avstånd. I enlighet med de allmänna principerna i lagen om militär underrättelseverksamhet ska åtgärderna vara förenliga med exempelvis proportionalitetsprincipen och principen om minsta olägenhet.

Vidtagandet av åtgärderna är bundet till nödvändighet. Med detta avses att militärunderrättelsemyndigheten inte hinner till platsen för att inleda användningen av metoden för underrättelseinhämtning. Ett exempel på detta är en situation där föremålet för militär underrättelseinhämtning kommer till ett gränsområde och systematisk spaning inte kan påbörjas, om inte en gränsbevakningsman i gränsområdet inleder sådan.

Med nödvändighet avses även att Gränsbevakningsväsendet utför åtgärden endast i den nödvändiga tiden, det vill säga att militärunderrättelsemyndigheten ska överta användningen av metoden för underrättelseinhämtning så fort som möjligt.

I paragrafens 1 mom. föreskrivs dessutom att Gränsbevakningsväsendet på begäran av en militärunderrättelsemyndighet utan obefogat dröjsmål ska avbryta en åtgärd som avses i detta moment, det vill säga så fort det är möjligt till exempel utan att äventyra syftet med användningen av metoden. En begäran om avbrytande kan bli aktuell till exempel i en situation där domstolen konstaterar att det inte hade funnits grunder som berättigar till ett tillstånd som gäller ett brådskande beslut om en metod för underrättelseinhämtning för militärunderrättelsemyndigheten. En begäran om avbrytande kan även göras utifrån ett meddelande av Gränsbevakningsväsendet, om Gränsbevakningsväsendet bedömer att det vid den ifrågavarande tidpunkten, till exempel på grund av de egna lagstadgade uppgifterna, inte har möjligheter att vidta den begärda åtgärden eller att fortsätta den eller om militärunderrättelsemyndigheten konstaterar att den själv har möjlighet att genomföra den begärda åtgärden. Nödvändigheten av att vidta åtgärden ska bedömas hela tiden.

Enligt föreslagna 2 mom. kan Gränsbevakningsväsendet på begäran av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman i samband med en uppgift som föreskrivs för Gränsbevakningsväsendet vidta sådana åtgärder som avses i 28 § i gränsbevakningslagen (578/2005) och som är nödvändiga med tanke på ett uppdrag inom den militära underrättelseinhämtningen. Det handlar alltså om hjälp som ges av Gränsbevakningsväsendet till militärunderrättelsemyndigheten och som utgör en form av mellanform mellan handräckning och samarbete, vilken främjar bland annat en förnuftig och effektivare resursanvändning vid myndigheterna. Gränsbevakningsväsendet använder sin specialkompetens och militärunderrättelsemyndigheten kan genom den mottagna information agera effektivare inom det egna specialkompetensområdet.

Utifrån momentet är det möjligt att vidta åtgärder i den omfattning som militärunderrättelsemyndighetens underrättelseuppdrag förutsätter och en förutsättning om nödvändighet fastställs för åtgärderna. Nödvändigheten ska bedömas med tanke på de i 1 mom. avsedda åtgärderna som ska vidtas, men även med tanke på om militärunderrättelsemyndigheten själv hinner till platsen för att använda metoder för underrättelseinhämtning.

Det bör observeras att Gränsbevakningsväsendet redan har en uppfattning av vem det lönar sig att välja till en närmare gränskontroll. Det kan förmodas att det även med tanke på Gränsbevakningsväsendets uppgifter är befogat att kontrollera personen i fråga, även om det primära behovet ser ut att anknyta till militär underrättelseinhämtning.

Det finns bestämmelser om befogenheterna för gränskontroll i 28 § i gränsbevakningslagen. I 1 mom. i paragrafen föreskrivs att en gränsbevakningsman för att genomföra gränskontroller

enligt gränskodexen för Schengenområdet, har rätt att utan brottsmisstanke vidta de åtgärder som räknas upp i 1–11 punkten i momentet i den omfattning som gränskodexen för Schengenområdet förutsätter. Enligt skäl 6 till kodexen om Schengengränserna bör gränskontroll bidra till kampen mot olaglig invandring och människohandel samt till förebyggande av alla typer av hot mot medlemsstaternas inre säkerhet, allmänna ordning, folkhälsa och internationella förbindelser.

Vid gränskontroll kan en gränskontroll i sin enklaste form utgöras av granskning av identiteten och resehandlingar och säkerställande av att de övriga förutsättningarna för inresa i landet är uppfyllda till exempel genom att ställa frågor om resans syfte och säkerställa att personen har tillräckliga medel för den meddelade vistelsetiden. Med den omfattning som det militära underrättelseuppdraget förutsätter avses att åtgärder enligt 28 § i gränsbevakningslagen, såsom en grundligare kontroll, vidtas i större omfattning än vad som i övrigt är behövligt till exempel i ett enskilt fall i gränskontrollen. Momentet begränsar inte Gränsbevakningsväsendets deltagande till endast uppgifter som genomförs i samband med gränskontrollen. Det är ändamålsenligt att Gränsbevakningsväsendet på begäran av en militärunderrättelsemyndighet kan genomföra de åtgärder som avses i 28 § även i samband med andra uppgifter, till exempel då det genomför kontroll i sjötrafiken eller fartygsinspektioner. Åtgärderna kan även till exempel handla om handlingar som innehas av en person, granskning av föremål som en person har med sig eller av ett fordon som han eller hon använder eller genomsökning av det eller kopiering av en persons resehandlingar, till exempel genom fotografering.

De åtgärder som vidtas ska alltid vara nödvändiga med tanke på militärunderrättelsemyndighetens underrättelseuppdrag. I bedömningen av nödvändigheten ska man beakta om den begärda åtgärden är nödvändig för underrättelseuppdraget och om det är nödvändigt att den vidtas av Gränsbevakningsväsendet så att militärunderrättelsemyndighetens uppdrag kan utföras framgångsrikt. Gränspasseringen kan vara den enda tillfället då egendom som innehas av föremålet för militär underrättelseinhämtning kan undersökas, oberoende av det handlar om dokument, informationsteknik eller ämnen. Nödvändighet kan innebära till exempel att en åtgärd som militärunderrättelsemyndigheten begär inte kan genomföras i ett annat sammanhang eller att militärunderrättelsemyndigheten i princip inte kan vidta den själv till exempel på grund av ärendets brådska. Gränsbevakningsväsendet har dessutom alltid möjlighet att vägra att vidta den begärda åtgärden, om det bedöms att det inte har de förutsättningar som behövs för att genomföra det eller om det kan äventyra utförandet av Gränsbevakningsväsendets egna lagstadgade uppgifter. Samverkan mellan Gränsbevakningsväsendet och militärunderrättelsemyndigheterna ska territoriellt sett riktas enligt 4 § i gränsbevakningslagen.

I paragrafens 2 mom. föreskrivs därtill att den person som är föremål för åtgärden är skyldig att vara närvarande högst 12 timmar åt gången när åtgärder vidtas och att beslut om vidtagande av en åtgärd ska fattas av chefen vid ett gränsövergångsställe eller en gränsbevakningsman med minst löjtnants grad. Eftersom momentet innehåller en hänvisning till de åtgärder som avses i 28 § i gränsbevakningslagen, för vilka en tid på högst tolv timmar har föreskrivits för Gränsbevakningsväsendet för att utföra dessa, är det ändamålsenligt att utfärda bestämmelser om att närvaroskyldigheten är lika lång. Det är möjligt att beslutet om åtgärder fattas av en gränsbevakningsman som fungerar som chef för gränsövergångsstället och en gränsbevakningsman med minst löjtnants grad, vilka i fråga om utbildning och erfarenhet kan anses ha tillräckliga färdigheter och kunskaper för att fatta beslutet.

Föreslagna 3 mom. i paragrafen innehåller rätt att i de föreskrivna situationerna enligt 2 mom. använda falska, vilseledande eller förtäckta uppgifter för att utföra åtgärder enligt 2 mom. då det är nödvändigt för att förhindra att åtgärden avslöjas. Utförandet av ett underrättelseuppdrag och inhämtandet av information av en militärunderrättelsemyndighet och de medel och metoder

som används i dessa ska kunna skyddas från att avslöjas även då Gränsbevakningsväsendet vidtar enskilda åtgärder i samband med den egna uppgiften. Syftet med användningen av falska, vilseledande eller förtäckta uppgifter är med andra ord ett behov av att man för föremålet för inhämtande av information inte avslöjar att en befogenhet som motsvarar en befogenhet som används i gränskontroll i verkligheten helt eller delvis används för underrättelseinhämtning. Gränsbevakningsväsendet är i så fall inte skyldigt att till exempel underrätta föremålet för åtgärden om det faktiska skäl som påverkar gränskontrollens omfattning. Det är möjligt att beslutet om skyddet fattas av en gränsbevakningsman som fungerar som chef för gränsövergångsstället och en gränsbevakningsman med minst löjtnants grad, vilka i fråga om utbildning och erfarenhet kan anses ha tillräckliga färdigheter och kunnande för att fatta beslutet.

Enligt paragrafens 4 mom. ska Gränsbevakningsväsendet lämna upptagningar och handlingar som fåtts genom en åtgärd som avses i denna paragraf obehandlade till militärunderrättelsemyndigheten samt utplåna upptagningar och handlingar som uppkommit vid genomförandet av åtgärden.

Eftersom Gränsbevakningsväsendet kan utföra de uppgifter som föreskrivs i denna paragraf i samband med en uppgift som föreskrivits för Gränsbevakningsväsendet, gäller utplåningsskyldigheten naturligtvis inte för sådana upptagningar och handlingar som Gränsbevakningsväsendet behöver för att utföra den egna uppgiften, även om de kan höra även till de upptagningar och handlingar som överläts till militärunderrättelsemyndigheten. Bägge myndigheter ansvarar då för att lagra uppgifterna och för att utplåna dem enligt den egna regleringen.

Gränsbevakningsväsendet har dock alltid rätt att i sitt eget register införa grundläggande uppgifter om tidpunkten och platsen för en åtgärd enligt denna paragraf och information om att en åtgärd har vidtagits eller inte har vidtagits.

20 §. Internationellt samarbete. Paragrafens 3 mom. ändras. Från bestämmelsen stryks hänvisningen till användningen av vissa metoder för underrättelseinhämtning. I och med att hänvisningen slopas kan en utländsk behörig myndighet delta i användningen av vilken som helst metod för underrättelseinhämtning i samarbete med en tjänsteman hos militärunderrättelsemyndigheten.

Det föreslås inte att den självständiga rätten för en utländska tjänsteman att agera i Finland utvidgas. Rätten för en behörig utländsk tjänsteman att delta i användningen av metoder för underrättelseinhämtning inom det finländska territoriet är fortfarande bunden till samarbete med militärunderrättelsemyndigheten. En utländsk tjänsteman har fortfarande inte självständig beslutanderätt eller självständig rätt att använda metoder för underrättelseinhämtning i Finland och man är inte på väg att ändra den verksamhetsmodell som redan tidigare beskrivits i den gällande lagen och regeringens proposition om lagen om militär underrättelseverksamhet, där militärunderrättelsemyndigheten har det övergripande ansvaret för en underrättelseoperation och lagenligheten för en enskild metod som används i den samt för styrningen och övervakningen.

Den utländska behöriga tjänstemannen fungerar fortfarande snarare i en biträdande roll i fråga om användningen av metoden, även om termen delta används i förslaget till bestämmelse. Alla åtgärder som avses i bestämmelsen sker under övervakning och styrning av en tjänsteman från militärunderrättelsemyndigheten. Syftet med ändringen är att säkerställa att militärunderrättelsemyndigheten och den utländska underrättelse- eller säkerhetstjänsten under den gemensamma operationen har tillgång till allt tekniskt och taktiskt kunnande samt de resurser

som den utländska underrättelse- eller säkerhetstjänsten har för att genomföra en enskild metod för underrättelseinhämtning. Det är behövligt att delta i användningen av metoden i synnerhet i det tekniska genomförandet av sådana metoder för tele- och datanätsunderrättelseinhämtning för vilka militärunderrättelsemyndigheten, på grund av den snabba tekniska utvecklingen eller teknikens unika karaktär, inte har utbildning, annan kompetens eller resurser, och ovan nämnda färdigheter inte kan skaffas inom tidsfönstret för att genomföra underrättelseuppdraget.

Deltagandet tillsammans med en tjänsteman hos militärunderrättelsemyndigheten ska bedömas enligt varje metod för underrättelseinhämtning. Till exempel vid underrättelseinhämtning som avser datatrafik kan deltagandet ske i den omedelbara närheten av en tjänsteman som tjänstgör för militärunderrättelsemyndigheten genom att ge tjänstemannen från militärunderrättelsemyndigheten råd som gäller analysen av uppgifterna och fastställandet av närmare sökbegrepp.

Å andra sidan kan en tjänsteman från militärunderrättelsemyndighet vid täckoperationer, på grund av deras natur, inte i alla situationer vara i den omedelbara närheten av en utländsk person som arbetar under en täckidentitet. Således kan en utländsk person som jobbar under täckmantel sköta sin uppgift i sig självständigt, men han eller hon ska iaktta de anvisningar, föreskrifter och andra begränsningar som getts av militärunderrättelsemyndigheten.

Som tredje exempel kan man även nämna teleavlyssning, där deltagandet kan innebära till exempel utnyttjande av sådana anordningar och metoder som militärunderrättelsemyndigheten inte har tillgång till. I dessa situationer kan statens tjänsteman till exempel vidta den egentliga tekniska åtgärden för underrättelseinhämtningen, men analysen av de inhämtande uppgifter sker av militärunderrättelsemyndigheten eller i samarbete med militärunderrättelsemyndigheten.

Med tanke på alla ovan beskrivna exempel är det centrala att verksamheten ska ske enligt Finlands nationella intressen, i anknytning till uppdragen i den militära underrättelseinhämtningen eller för att trygga den nationella säkerheten. I varje fall har en utländsk tjänsteman vid verksamhet enligt bestämmelsen inte någon självständig befogenhet till underrättelseinhämtning i Finland. Om en utländsk tjänsteman agerar på annat sätt än vad som konstaterats i bestämmelsen, gör han eller hon sig skyldig till brott.

Med tanke på bestämmelsen är det centralt att en utländsk tjänsteman är skyldig att iaktta de föreskrifter, begränsningar och anvisningar vilka en militärunderrättelsemyndighet gett honom eller henne. Om en utländsk tjänsteman inte iakttar dessa, kan han eller hon göra sig skyldig till ett brott som föreskrivits som ett brott i strafflagen, såsom spionage eller olovlig underrättelseverksamhet. Tjänsteansvaret för en utländsk tjänsteman regleras separat i 21 § i lagen. Dessutom bör det observeras att om en utländsk tjänsteman förfar i strid med vad som föreskrivits i 20 § 3 mom. i lagen eller en utländsk underrättelse- eller säkerhetstjänst förfar egenmäktigt på det finska territoriet, handlar det om brottslig verksamhet.

I enlighet med den föreslagna ändringen har militärunderrättelsemyndigheten en särskild skyldighet att utreda de risker som orsakas av verksamheten, skyddet för de grundläggande fri- och rättigheter och de mänskliga rättigheter vilka grundlagen skyddar samt tillgodoseendet av de allmänna principerna i lagen om militär underrättelseverksamhet innan militärunderrättelsemyndigheten fattar ett beslut om att en utländsk behörig tjänsteman deltar i användningen av metoder för underrättelseinhämtning.

Militärunderrättelsemyndigheten ska dessutom informera en samarbetande underrättelse- och säkerhetstjänst om den utländska tjänstemannens tjänsteansvar i anknytning till samarbetet och

styrningen och övervakningen ska ordnas på ett sätt som gör att det är möjligt att på ett tillräckligt sätt säkerställa lagenligheten i den utländska tjänstemannens verksamhet.

Övervakning av internationellt samarbete omfattas av underrättelsetillsynsombudsmannens behörighet på samma sätt som även annan militär underrättelseverksamhet.

33 §. Beslut om teknisk observation av utrustning. Till 2 punkten i paragrafens 3 mom. fogas en hänvisning till en person som använder en teknisk anordning eller programvara. På samma sätt som i fråga om många andra metoder för underrättelseinhämtning, ska även teknisk observation av utrustning kunna riktas på personbasis.

När ett tillstånd till teknisk observation av utrustning hänför sig till en person, omfattar tillståndet en anordning eller en programvara som innehas av den person som är föremål för tillståndet eller som i övrigt enligt förmodan används av honom eller henne. Ett tillstånd till teknisk observation av utrustning är inte anordnings- eller programvaruspecifikt, utan tillståndet omfattar alla anordningar och programvaror som innehas och används av den person som är föremål för tillståndet. Innehavaren av tillståndet ska kunna påvisa grunder för att en viss person som är föremål för tillståndet är delaktig i verksamhet som är föremål för den militära underrättelseinhämtning eller verksamhet som allvarligt hotar den nationella säkerheten. Vid teknisk observation av utrustning som riktar sig mot en person kan inhämtandet av information vara ett komplement till övriga metoder för underrättelseinhämtning. När den person som är föremål för en åtgärd som fastställs i ett domstolstillstånd tar i bruk eller förmodas ha tagit i bruk nya anordningar eller programvaror eller då det kommer fram att han eller hon innehar en anordning eller använder en programvara, kan underrättelsemyndigheten rikta en åtgärd mot dessa anordningar och programvaror. När nya anordningar och programvaror fogas till ett tillstånd, ska man även i fråga om dessa fatta ett myndighetsbeslut och göra en anmälan till underrättelseombudsmannen.

På samma sätt som i fråga om andra metoder för underrättelseinhämtning som hänför sig till en person, föreskrivs i paragrafens 4 mom. att man under tiden för användningen av en metod för underrättelseinhämtning fattar ett myndighetsbeslut om att lägga till en ny anordning eller programvara som föremål för användningen av metoden. När ett nytt tillstånd eventuellt ansöks för teknisk observation av utrustning från en domstol, ska de identifierade anordningarna och programvarorna anmälas i yrkandet på ett sätt som motsvarar det nuvarande förfarandet i fråga om metoder för underrättelseinhämtning som hänför sig till en person.

36 §. Beslut om teleavlyssning och annat motsvarande inhämtande av information. Till paragrafens 1 mom. fogas en möjlighet till ett akut beslut på ett sätt som motsvarar vad som föreskrivits exempelvis om teleavlyssning (38 §) och egentlig underrättelseinhämtning som avser data trafik (69 och 71 §). Det akuta förfarandet kan anses vara exceptionellt, eftersom domstolen har ett fungerande joursystem.

Om en domstol i samband med ett beslut som fattats i en brådskande situation anser att förutsättningar för åtgärden inte förelegat, ska användningen av metoden för underrättelseinhämtning avslutas och det material och de anteckningar om de uppgifter som fåtts genom den direkt utplånas.

Ett ärende som gäller akuta beslut ska hänskjutas till domstol trots att teleavlyssning eller annat motsvarande inhämtande av information avslutas inom 24 timmar från det att metoden började användas. I annat fall är det möjligt att genom kortvarigt inhämtande av information kringgå de krav som ställts på förfarandet för beslutsfattande. Ett lagenligt förfarande främjas av att ärendet hänskjuts till domstol även i sådana fall. Detta gäller även för andra situationer där en med

användningen av metoder för underrättelseinhämtning vid militärunderrättelsemyndigheten särskilt förtrogen militärjurist eller annan tjänsteman tillfälligt kan fatta beslut om användningen av metoden för underrättelseinhämtning.

På samma sätt som i fråga om andra metoder för underrättelseinhämtning som hänför sig till en person, föreskrivs i paragrafens 4 mom. att man under tiden för användningen av en metod för underrättelseinhämtning fattar ett myndighetsbeslut om att lägga till en ny anordning eller programvara som föremål för användningen av metoden. När ett nytt tillstånd eventuellt ansöks för teknisk observation av utrustning från en domstol, ska de identifierade anordningarna och programvarorna anmälas i yrkandet på ett sätt som motsvarar det nuvarande förfarandet i fråga om metoder för underrättelseinhämtning som hänför sig till en person.

42 §. *Installation och avinstallation av anordningar, metoder eller programvara.* I paragrafens 1 mom. görs en teknisk ändring genom att till listan över metoder för underrättelseinhämtning foga underrättelseinhämtning i hemlandet som avser statliga aktörers datasystem och underrättelseinhämtning som avser utländska datasystem.

Paragrafens 2 mom. är nytt. Enligt det kan militärunderrättelsemyndigheten begära att en person som inte hör till myndigheten vidtar en enskild installations- eller avinstallationsåtgärd för att uppnå de mål som avses i paragrafen. De situationer som avses i bestämmelsen handlar om åtgärder som en militärunderrättelsemyndighet inte själv kan vidta i den rådande situationen, även om myndigheten har en befogenhet till detta. Det står klart att myndigheten i princip på egen hand ska vidta de åtgärder som avses i paragrafens 1 mom. och endast i nödvändiga fall kan myndigheten förlita sig på hjälp av en extern aktör. Nödvändighetskravet innebär i princip att det är möjligt att visa att användningen av den metod för underrättelseinhämtning till vilken exempelvis installationen anknyter inte är möjlig eller åtminstone kräver väsentligt mer resurser eller fördröjer inhämtningen av information på ett oskäligt sätt med hänsyn till hotets allvar.

Verksamhet enligt bestämmelsen baserar sig på en begäran som framförs av en myndighet och mottagaren av begäran har rätt att vägra att tillmötesgå begäran. Ett svar ska ha getts frivilligt innan en åtgärd vidtas och mottagaren av begäran ska ha förstått dess betydelse. Svaret ska vara genuint frivilligt. Den som framför en begäran får inte övertala eller på annat sätt leda en extern aktör till det önskade svaret. Det är ändamålsenligt att underrättelsemyndigheten för fram att ett samtycke ligger till grund för åtgärden, men den berörda personen ska själv få dra slutsatser om vidtagandet av åtgärder. Eventuella konsekvenser som kan drabba ett biträde ska även föras fram till honom eller henne. I princip handlar det om verksamhet som sker inom ramen för myndighetens befogenhet, till vilken myndigheten också själv har rätt. Således kan biståndet till en myndighet i sig inte vara en uppsägningsgrund. Om ett biträde förfar i strid med de noggranna anvisningar som getts honom eller henne, kan detta naturligtvis i sista hand leda till uppsägningen.

Den åtgärd som avses i bestämmelsen är avgränsad till det noggrant avgränsade objekt som angetts av militärunderrättelsemyndigheten och åtgärden ska vidtas enligt militärunderrättelsemyndighetens anvisningar. Redan på grund av risken för att verksamheten avslöjas ska militärunderrättelsemyndigheten kunna lita på att den biträdande personen förfar enligt anvisningarna. I det lindrigaste fallet kan till exempel bistånd för att installera utrustning innebära till exempel att biträdet för en låda innehållande en viss utrustning till en viss fastställd plats till vilken han eller hon har tillträde.

En sådan åtgärd som avses i paragrafen handlar om en så kallad sidobefogenhet, det vill säga att den har en fast koppling till den använda metoden för underrättelseinhämtning och till hur användningen av respektive metod för underrättelseinhämtning har avgränsats. Till exempel om

det handlar om teknisk avlyssning, kan det handla om installation av en mikrofon i ett visst utrymme.

Vid teknisk observation av utrustning kan det handla om installation av en bevakande programvara i en viss utrustning eller programvara. I ett yrkande på tillstånd som gäller teknisk observation av utrustning ska man noggrant specificera den utrustning eller programvara, varför det utifrån den nu behandlade bestämmelsen inte är möjligt att installera exempelvis anordningar som möjliggör massövervakning i teleoperatörers utrymmen. Inte heller för detta finns det någon befogenhet.

Installations- och avinstallationsåtgärder ska således riktas endast till en specificerad och avgränsad anordning, metod eller programvara i enlighet med metoden för underrättelseinhämtning. Det är inte möjligt att utsträcka åtgärderna till exempel till ett teleföretags centrala hanterings-, övervakning- eller andra kärnsystem i andra än exceptionella fall och utifrån synnerligen vägande grunder och även då i så begränsad form som möjligt. Dessutom ska åtgärderna planeras på så sätt att de inte orsakar exempelvis observation om avvikelser eller automatiska skyddsåtgärder i ett teleföretags övervaknings- och störningshanteringssystem. Detta är nödvändigt för såväl driftsäkerheten som den operativa säkerheten. I synnerhet militärunderrättelsemyndighetens operationssäkerhet styr till att vidta åtgärderna på så sätt att administratören av målsystemet inte upptäcker åtgärderna.

Dessutom är detta av betydelse för ett eventuellt skadestånd. Om ett biträde förfar noggrant enligt militärunderrättelsemyndighetens anvisningar, handlar det om verksamhet som sker på myndighetens ansvar, det vill säga att ett eventuellt skadeståndsansvar hänförs till myndigheten. Situationen motsvarar en situation där myndigheten själv vidtar åtgärden på plats, vilket eventuellt orsakar oförutsedda skador.

Om ett biträde instruerats att installera en USB-enhet med vilken en programvara som möjliggör teknisk observation av utrustning installeras i en anordning, sker detta i praktiken tydligt inom ramen för myndighetens befogenheter och om installationen eller den tekniska observationen av utrustning orsakar skada för en utomstående, ansvarar myndigheten för detta på samma sätt som myndigheten hade själv hade gjort installationen.

Om biträdet förfar enligt egen prövning i strid med de mottagna anvisningarna, ansvarar biträdet själv för eventuella skador. Situationen motsvarar till stor del att en styrd informationskälla orsakar skador eller begår brott i samband med ett tilldelat underrättelseuppdrag.

Framför allt noggrann planering, noggranna anvisningar till ett biträde samt riskbedömningen betonas i varje fall i vidtagandet av en åtgärd. Naturligtvis styrs verksamheten även av att den militära underrättelseverksamheten ska hållas hemlig och av ett starkt förtroende för biträdet.

I fråga om en metod för underrättelseinhämtning som möjliggör installation ska de föreskrivna förutsättningarna för detta vara uppfyllda – naturligtvis ska det föreskrivna förfarandet för beslutsfattande med tillstånd iaktas i fråga om dessa. En i bestämmelsen avsedd informationskälla får inte användas för att kringgå de begränsningar som gäller användningen av de befogenheter som tilldelats myndigheter. Användningen av ett biträde ska redogöras i ett beslut som gäller användningen av en metod för underrättelseinhämtning. I varje fall ska militärunderrättelsemyndigheten fatta ett beslut om den verksamhet som avses i paragrafen och underrätta underrättelsetillsynsombudsmannen om det. Dessutom övervakar underrättelsetillsynsombudsmannen verksamhet enligt sin befogenhet.

Dessutom ska åtgärden basera sig på ett beslut om att använda metoden för underrättelseinhämtning, vilket har fattats på behörigt sätt av myndigheten. Det står klart att en myndighet med stöd av bestämmelsen inte kan begära att en person gör ospecificerade installationer av de anordningar, metoder eller programvaror som avses i paragrafen med en förmodan om att de i något skede kan bli användbara.

På grund av det ovan konstaterade handlar det om verksamhet av engångskaraktär. Således kan en begäran av en myndighet och svaret på den inte vara av permanent natur, utan det handlar alltid om att en enskild åtgärd vidtas.

Verksamheten enligt bestämmelsen sker inom ramen för myndighetens befogenhet och under dess uppsikt och övervakning. Åtgärderna handlar alltid om åtgärder som myndigheten enligt lag har möjlighet att vidta. Biträdet genomför inte inhämtande av information utan till exempel den tekniska hanteringen av en anordning, styrningen av dess funktion, granskningen av upptagningar och bedömningen ankommer fortsättningsvis på den behöriga myndigheten. De åtgärder som vidtas kan inte anses innebära utövning av offentlig makt.

Begränsningarna i paragrafens 1 mom. tillämpas även på åtgärder som vidtagits av en person som inte hör till myndigheten, varför installations- och avinstallationsåtgärder inte får göras i ett utrymme som används för boende av permanent natur.

Det ovan konstaterade leder även till att ett biträde inte kan vidta åtgärder i ett utrymme som används för boende av permanent natur, så som föreskrivits uttryckligen i paragrafens 1 mom.

Även installation av en anordning, metod eller programvara är centralt med tanke på bestämmelsen. Avinstallationen ska bedömas med tanke på nödvändigheten, det vill säga att en anordning, metod eller programvara ska vara installerad endast i den nödvändiga tiden. Till exempel med tanke på den installerade programvaran ska den eventuella dataskyddsriskerna för den anordning som utgör objekt bli så liten som möjligt.

Paragrafens 3 mom. är nytt. I enlighet med paragrafens 1 mom. har en myndighet för installation, ibruktagande och avinstallation rätt att i hemlighet ta sig in i ovannämnda objekt och i ett informationssystem och att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektets eller informationssystemets säkerhetssystem. För att ta sig in i ett informationssystem och till exempel passera skyddet i ett informationssystem kan det vara nödvändigt att i smyg sticka in den behövliga programvaran med en fjärranslutning genom att använda externa informationssystem och anordningar. I verksamheten ska man naturligtvis undvika att orsaka skada för de använda systemen och anordningarna och undvika att de externa informationssystemen och anordningarna avslöjas för objektet.

Enligt den nya bestämmelsen kan militärunderrättelsemyndigheten i hemlighet använda även externa anordningar och informationssystem. Bestämmelsen avgränsar installation och avinstallation samt informationsförmedling till datatekniska metoder, det vill säga att militärunderrättelsemyndighetens tjänsteman inte fysiskt sett vidtar några åtgärder i anordningen eller datasystemet, utan det handlar uttryckligen om att installera och avinstallera en metod eller programvara på distans genom datatekniska metoder.

Till exempel kan objektet för militär underrättelseinhämtning själv använda sådana externa anordningar eller datasystem, varvid militärunderrättelsemyndigheten har möjlighet att få ett grepp om objektet via denna externa anordning eller detta externa datasystem. En sådan situation kan föreligga om objektet för militär underrättelseinhämtning drar nytta av till exempel nätet vid ett café eller köpcentrum, varvid det naturligaste för militärunderrättelsemyndigheten

är att utnyttja samma nät för att vidta de behövliga åtgärderna i anordningarna för objektet för militär underrättelseinhämtning.

Med beaktande av målet med bestämmelsen, kan installationen och avinstallationen en anordning, metod och programvara samt informationsförmedlingen i praktiken inte ske till exempel i ett teleföretags kritiska produktionsmiljö. Även i detta fall handlar det om en relativt resurskrävande åtgärd, och därtill får åtgärden inte på något sätt synas för det egentliga föremålet. Detta orsakar en tämligen stor risk för att systemets funktion störs på så sätt att det väcker föremålets intresse.

Utöver det ovan konstaterade ska det beaktas att lagens allmänna principer tillämpas även på de åtgärder som avses i paragrafen, vilka har en fast koppling till användningen av den egentliga metoden för underrättelseinhämtning. Således leder redan exempelvis principen om minsta olägenhet till att utnyttjande av mer omfattande datanätshelheter eller informationssystemshelheter i praktiken inte blir aktuella. Dessutom leder proportionalitetsprincipen till att de åtgärder som vidtas ska vara proportionella i förhållande till den använda metoden för underrättelseinhämtning och underrättelseuppdragets mål. Med tanke på principerna kan användningen av ett teleföretags kritiska produktionsmiljö i ovan avsedda exempel för verksamheten enligt bestämmelse i praktiken anses utgöra ett teoretiskt alternativ.

Installationen och avinstallationen ska i regel ske så nära objektet som möjligt, såsom genom ett allmänt delat trådlöst nät i ett café i ovan beskrivna fall. Om det handlar om fysiska åtgärder som gäller installation eller avinstallation, blir 1 mom. eller 2 mom. i paragrafen tillämpligt.

Bestämmelsen avgränsar åtgärden till enskilda utrustningar eller en del av ett informationssystem. Således ska militärunderrättelsemyndigheten kunna identifiera den anordning eller del av ett informationssystem via vilken metoden eller programvaran kan installeras i objektet. Det är inte ändamålsenligt att utsträcka åtgärderna till exempel till ett teleföretags centrala hanterings-, övervakning- eller andra kärnsystem i andra än exceptionella fall och utifrån synnerligen vägande grunder och även då i så begränsad form som möjligt.

De avsedda åtgärderna handlar inte heller om att exempelvis tillverkaren av en anordning färdigt ska installera en programvara eller en metod som möjliggör användning av metoder för underrättelseinhämtning i de anordningar som den säljer.

Nödvändighet är en förutsättning för verksamhet enligt bestämmelsen. I vissa fall handlar det om att bedöma om militärunderrättelsemyndigheten kan uppnå det önskade målet genom egna åtgärder utan att använda externa anordningar eller informationssystem. Om de egna åtgärderna är omöjliga eller kräver exceptionellt stora resurser, uppfylls det krav på nödvändighet som avses i bestämmelsen. Nödvändigheten ska bedömas även med tanke på den anordning eller del av ett informationssystem som används i installationen, avinstallationen eller dataöverföringen. Användning av exempelvis ett allmänt öppet delat nät kan bli aktuellt med en lägre tröskel, medan användning av en signifikativare kraftigt skyddad anordning eller del av ett datasystem vid åtgärden inte blir aktuellt lika ofta. I den sist nämnda situationen ska man bedöma om åtgärden kan vidtas via en utrustning eller en del av ett informationssystem som kräver mindre resurser eller eventuellt orsakar mindre skador.

I bedömningen ska man bedöma även den övergripande betydelsen för den anordning eller del av informationssystemet som är föremål för åtgärden. Till exempel en störning i en enskild anordning kan orsaka följdverkningar som till och med kan vara avsevärda, om det handlar om en anordning som är centralt för det kommunikationsnät som administreras av ett teleföretag.

Det är väldigt sällsynt att bestämmelsen tillämpas i fråga om sådana anordningar. På grund av de allmänna principerna för militär underrättelseverksamhet och sekretessbeläggningen försöker man hålla den mängd data som rör sig via enskilda anordningar eller informationssystem så osynlig som möjligt.

Den tillfälliga karaktär till vilken det hänvisas i bestämmelsen innebär att man i installationen och avinstallationen av en metod eller programvara och överföringen av data inte kan använda samma anordningar och informationssystem på permanent sätt. Ur en operativ synvinkel är det även ändamålsenligt att metoden eller programvaran i mån av möjlighet nästlas in i objektet genom att använda flera olika rutter samtidigt.

På grund av naturen på militärunderrättelsemyndighetens verksamhet är målet att göra installationen och avinstallationen och överföringen av data så obemärkt som möjligt. Även om man i verksamheten använder externa anordningar och informationssystem, försöker man således dölja spåren så grundligt som möjligt. Verksamheten handlar inte heller om att särskilda ändringar görs i en anordning eller ett datasystem som fungerar som förmedlare.

I enlighet med bestämmelsen är det i verksamheten inte tillåtet att orsaka större olägenhet än ringa för den anordning eller det informationssystem som används. Sådan verksamhet som avses i bestämmelsen handlar framför allt om att förmedla datatrafik för att installera eller avinstallera en metod eller en programvara och å andra sidan om överföring av data från objektets anordning eller system till militärunderrättelsemyndigheten. Således handlar en behövlig ringa olägenhet främst om tillfällig ökad användning av en datatrafikförbindelse och därmed om eventuell tillfällig långsammare funktion i de elektroniska tjänster som innehavaren av ett abonnemang använder. Användningen av ett externt informationssystem kan synas som en tillfällig uppgång i användningen av systemet.

I bedömningen av olägenheten ska man uttryckligen beakta eventuella konsekvenser för prestandan, såsom dröjsmålet och kapaciteten, de påföljder som orsakas för ägaren av överträdelsen av servicenivåavtalen, det extra arbetet för att utreda störningen, återställningsåtgärderna och anseendeolägenheten. Till exempel i teleföretagsmiljön är långsammare trafik eller sämre servicekvalitet i typfallet en större olägenhet än ringa.

Ovan konstaterade omständigheter ska beaktas i planeringen av åtgärderna i bestämmelsen, även om bestämmelsen inte handlar om storskalig verksamhet i fråga om en enskild datatrafikförbindelse. Eftersom åtgärderna inte handlar om till exempel åtgärder som riktar sig mot ett teleföretags kritiska produktionsmiljö och metoder och programvaror som installeras i princip är osynliga och man strävar efter att överföra information på ett obemärkt sätt, kan ovan beskrivna betydande konsekvenser i varje fall i praktiken bedömas vara teoretiska. Det sist nämnda skulle förutsätta att stora datamängder överförs via enskilda anslutningar.

Om en onödig olägenhet i strid med vad som beskrivits ovan orsakas av verksamheten enligt bestämmelsen, är militärunderrättelsemyndigheten skyldig att ersätta skadan och olägenheten. På grund av verksamhetens natur får den person eller den sammanslutning vars anordning eller informationssystem används inte information om militärunderrättelsemyndighetens verksamhet. Å andra sidan borde personen eller sammanslutningen i princip inte ens upptäcka något sådant. Om en person eller en sammanslutning misstänker att en anordning eller ett informationssystem använts på det sätt som avses i bestämmelsen och att instansen orsakats en större olägenhet än ringa av militärunderrättelsemyndighetens verksamhet, kan personen eller sammanslutningen framföra en begäran om undersökning till underrättelsetillsynsombudsmannen.

I sig står det klart att det i ovan beskrivna verksamhet inte är möjligt att inhämta information från en anordning eller ett informationssystem som utgör förmedlare eller från de uppgifter som dessa producerar. I så fall handlar det om inhämtande av information, vilket den aktuella bestämmelsen inte täcker. Genom att förfara på ovan avsedda sätt gör sig militärunderrättelsemyndigheten skyldig till brottslig verksamhet, om de tillstånd som behövs för att använda metoden för underrättelseinhämtning inte finns.

Momentets slut innehåller en informativ bestämmelse om att en militärunderrättelsemyndighet är skyldig att ersätta en större än ringa olägenhet eller skada som den orsakat. Skadestånd och processen för skadestånd föreskrivs i skadeståndslagen.

43 §. Täckoperation. Paragrafens 3 mom. upphävs. Momentet gäller täckoperationer i datanät, vilka föreskrivs i föreslagna 46 a § och i 46 b §, som gäller avbrytande av sådana operationer. På grund av detta är momentet onödigt.

Till övriga delar bibehålls paragrafen i oförändrad form och det anknutna rättsläget ändras inte.

44 §. Plan för en täckoperation. Paragrafen och dess rubrik ändras för att gälla endast en plan för en täckoperation. Beslutsfattandet om täckoperationer baserar sig alltid på en framställning, i vilken fakta som berör beslutet om täckoperationer ska inkluderas. Framställningen baserar sig alltid på en plan, som finns som bilaga till beslutshandlingarna, varför det kan anses vara onödigt att utfärda bestämmelser om en separat framställning.

45 §. Beslut om en täckoperation. Från paragrafens 1 mom. stryks hänvisningen till en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vilken förordnas till uppdraget och i praktiken beslutat om täckoperationer i datanät. Hänvisningen är onödig, eftersom man i propositionen föreslår att bestämmelser utfärdas om en uttrycklig befogenhet som gäller täckoperationer som genomförs uteslutande i datanät.

Från paragrafens 4 mom. stryks hänvisningen till avslutande av en täckoperation. Det kan anses vara onödigt att utfärda uttryckliga bestämmelser om avslutande, eftersom metoden för underrättelseinhämtning, på samma sätt som även andra metoder för underrättelseinhämtning, ska avslutas, om förutsättningar inte längre föreligger för en sådan.

46 a §. Täckoperation som genomförs uteslutande i datanät. Till lagen fogas en ny paragraf som innehåller bestämmelser om en befogenhet till täckoperationer som genomförs uteslutande i datanät. Det är motiverat att utfärda separata uttryckliga bestämmelser om befogenheten för en täckoperation på grund av dess låga användningströskel. De hot som är föremål för militär underrättelseinhämtning behandlas ofta även i datanät och inhämtande av närmare information om hot förutsätter ofta umgänge till exempel med personer som deltar i en diskussion. Med tanke på militär underrättelseinhämtning är det dessutom alltid säkrare att inhämta information från Finland jämfört med att fysiskt åka till målstaten. Metoden är även av betydelse för att hitta nya objekt.

Det föreslås att paragrafens 1 mom. innehåller bestämmelser om definitionen av täckoperationer som uteslutande genomförs i datanät. Med täckoperation avses planmässigt inhämtande av information om en viss person eller om personens 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. Definitionsbestämmelsen förutsätter inte att den person eller grupp av personer som är föremål för åtgärden kan namnges eller specificeras till exempel enligt deras egenskaper, utan det räcker att personen eller gruppen

av personer kan specificeras till exempel genom den verksamhet som bedrivs. Eftersom ett av målen med täckoperationer är att utreda de strukturer som anknyter till målverksamheten och de personer som verkar i dessa, är det inte befogat att en förutsättning för sådant utredningsarbete är information om till exempel personens namn.

Definitionsmässigt motsvarar täckoperationer som genomförs uteslutande i datanät vad som i 43 § i lagen föreskrivs om normala täckoperationer och vad som i 43 § 3 mom. föreskrivs om täckoperationer i datanät.

I 2 mom. föreskrivs om en särskild förutsättning för befogenheten. Förutsättningen motsvarar vad som föreskrivs i 43 § 3 mom. i den gällande lagen. Täckoperationer som genomförs uteslutande i datanät är möjliga, om de kan antas vara av synnerlig vikt med avseende på ett underrättelseuppdrag.

Det föreslås att paragrafens 3 mom. innehåller bestämmelser om en plan för täckoperationer som genomförs uteslutande i datanät. Den ska innehålla väsentliga och tillräckligt detaljerade uppgifter för beslutsfattandet och genomförandet av täckoperationen. Vid behov ska en plan ses över

46 b §. *Beslut om en täckoperation som genomförs uteslutande i datanät.* Paragrafen innehåller bestämmelser om beslutsfattandet. Beslutsfattandet motsvarar vad som tidigare beslutats om en täckoperation som genomförs i datanät med stöd av 45 § i lagen.

Enligt paragrafens 1 mom. fattas ett beslut av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Nivån på beslutsfattandet motsvarar vad som för närvarande iakttas i fråga om täckoperationer som genomförs i datanät enligt 45 § i lagen.

Enligt 2 mom. i paragrafen kan ett beslut vara i kraft i högst sex månader åt gången. Enligt paragrafens 3 mom. ska ett beslut fattas skriftligen.

Paragrafens 4 mom. innehåller bestämmelser om de omständigheter som ska nämnas i ett beslut. De omständigheter som nämns i ett beslut motsvarar vad som föreskrivits i 45 § i lagen. Befogenheten hänför sig framför allt till verksamheten i anknytning till ett hot, vilken definierats noggrannare i underrättelseuppdraget. Vid förfarande i ett datanät kan det i praktiken vara omöjligt att fastställa en viss målperson, eftersom det är möjligt att personer dyker upp i snabb takt till exempel i en diskussion och å andra sidan kan de även avlägsna sig från diskussionen lika snabbt. I ett underrättelseuppdrag ska man dock kunna avgränsa målverksamheten så noggrant som möjligt och täckoperationer som genomförs i datanät kan inte vara helt oriktade.

51 §. *Användning av informationskällor.* Paragrafens 3 mom. delas upp i nya 3 och 4 mom. Gällande 3 mom. kan anses vara oklart för dem som tillämpar bestämmelsen. Ändringen har även konsekvenser för underrättelseinhämtning som görs utomlands.

Nya 3 mom. gäller det förbud som tillämpas vid styrd användning av informationskällor, vilket gäller inhämtande av information på ett sådant sätt som förutsätter att befogenheter som hör till en myndighet utövas. I praktiken har detta inneburit att en informationskälla inte kan skaffa sådana uppgifter till vilka källan inte har tillträde. Om en informationskälla beviljats rätt att använda uppgifter i en viss mapp i ett visst datasystem, kan informationskällan överlämna endast dessa uppgifter till underrättelsemyndigheten. Informationskällan har dock inte rätt att gå in och inhämta uppgifter ur uppgifter som används av en person med andra behörigheter, vilket redan skulle innebära utövning av myndighetsbefogenheter.

I och med ändringen förs ovan avsedda regel fram tydligare och den föreskrivs i ett separat moment.

Det föreslås att paragrafens nya 4 mom. innehåller bestämmelser om redogörelse för rättigheterna och skyldigheterna för en informationskälla och omständigheter som gäller en informationskällas säkerhet. Momentet innehåller de övriga ärenden som föreskrivs i 3 mom. i den gällande lagen än de som enligt förslaget föreskrivs i nya 3 mom. Till dessa delar påverkar ändringen inte det gällande rättsläget.

I och med den föreslagna ändringen övergår 4 och 5 mom. i den gällande paragrafen till att bli nya 5 och 6 mom.

53 §. Beslut om styrd användning av informationskällor. I paragrafens 1 mom. görs en teknisk ändring. I och med ändringen kan även en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman fatta beslut om styrd användning av informationskällor. Ändringen motsvarar vad som föreskrivits i 5 a kap. i polislagen om beslut om styrd användning av informationskällor vid skyddspolisens.

Ändringen är behövlig, eftersom beslutsfattarnivån sänks till en nivå som ligger närmare den operativa verksamheten. Således är det möjligt att vid styrd användning av informationskällor bättre reagera på situationer som förändras snabbare. En beslutsfattare som finns på lägre nivå och närmare den operativa verksamheten kan även bedömas ha bättre information om själva verksamheten till stöd för beslutsfattandet.

55 §. Beslut om platsspecifik underrättelseinhämtning. I paragrafens 3 mom. görs en teknisk ändring. I och med ändringen fattas ett beslut om platsspecifik underrättelseinhämtning i ett fordon av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Ett fordon är en plats dit man inte har allmänt tillträde vid tidpunkten för platsspecifik underrättelseinhämtning, men det inte är befogat att det ger likadant skydd som exempelvis ett låst kontor i en normal situation. Genom ändringen av beslutsfattandet är det inte behövligt att ett beslut om platsspecifik underrättelseinhämtning som avser ett fordon fattas i domstol. Beslutsfattandet motsvarar vad som i tvångsmedelslagen föreskrivits om genomsökning av platser.

Vid tillämpningen av bestämmelsen ska man dock beakta situationer där ett fordon används för boende av permanent natur.

55 a §. Provtagning vid platsspecifik underrättelseinhämtning. Paragrafen är ny. Enligt bestämmelsen har en militärunderrättelsemyndighet rätt att vid platsspecifik underrättelseinhämtning ta prover från ett ämne, egendom eller ett föremål, om det behövs för utförandet av underrättelseuppdraget. I och med bestämmelsen kan en militärunderrättelsemyndighet i samband med användningen av en metod för underrättelseinhämtning ta prover till exempel från ett ämne, som kan förmodas vara kopplat till den verksamhet som är föremål för underrättelseuppdraget.

56 a §. Tillfälligt omhändertagande av ämnen, egendom eller föremål. Enligt 4 § i lagen utgörs föremålen för militär underrättelseinhämtning av bland annat militär verksamhet, underrättelseverksamhet som riktar sig mot Finlands försvar och en främmande stats verksamhet eller någon annan sådan verksamhet som allvarligt hotar det finska försvaret eller som äventyrar samhällets vitala funktioner. Det är uppenbart att då den ovan avsedda

verksamheten tar sig i uttryck i nya former i den rådande världspolitiska situationen, kan man till exempel i samband med platsspecifik underrättelseinhämtning hitta sådana ämnen som eventuellt kan användas för att tillverka sprängmedel eller till exempel giftiga kemikalier. I allmänhet är det dock inte möjligt att identifiera ett ämne som hittats och inte heller att bedöma dess farlighet enbart utifrån de externa kännetecknen. I anknytning till utländsk underrättelseverksamhet kan det handla om en situation där text skrivits med ett kemiskt ämne på upphittade handlingar på ett sätt som inte syns med blotta ögat och texten kan göras synlig endast genom att använda ett annat ämne.

Även om man i princip i dessa situationer kan förmoda att det handlar om verksamhet som uppfyller ett brottsrekvisit, är det inte möjligt att få visshet om till exempel ämnets art förrän man gjort noggrannare tester. Om sådan information som inhämtats med stöd av befogenheten i paragrafen avseende till exempel ett ämne som används i ett sprängmedel bekräftas, kan informationen lämnas ut i enlighet med den så kallade brandväggsregleringen till brottsbekämpningsmyndigheten.

På grund av underrättelseverksamhetens natur är det omhändertagande som avses vid användningen av befogenheten tillfälligt. För att militärunderrättelsemyndighetens verksamhet ska hållas hemlig, ska omhändertagandet vara så kortvarigt som möjligt, och det ämne, det föremål eller den egendom som omhändertas ska returneras så fort som möjligt till den ursprungliga platsen.

61 a §. *Underrättelseinhämtning i hemlandet som avser statliga aktörers datasystem.* Det föreslås att paragrafen innehåller bestämmelser om ny underrättelseinhämtning i Finland, vilken avser statliga aktörers datasystem. I lagen har en statlig aktör definierats som en identifierad myndighet i en främmande stat eller en jämförbar aktör och en aktör som tjänstgör för en ovan avsedd aktör eller under dess order och handledning.

Med datasystem avses en helhet som utgörs av anordningar för informationsbehandling, anordningar för informationsöverföring, program för informationsbehandling och protokoll för behandling av uppgifter. Ett datasystem kan utgöras av en geografiskt och logiskt utspridd helhet som består av flera olika anordningar och programvaror eller delar av dessa. Datasystemet kan täcka delar som samtidigt hör till något annat datasystem.

Underrättelseinhämtning som avser datatrafik enligt paragrafen innehåller tekniskt sett metoder som motsvarar teleavlyssning och teleövervakning samt teknisk observation av utrustning och kombinationer av dessa, med vilka det är möjligt att inhämta information om ett meddelande som rör sig i informationssystemet, lagrats i det och uppgifter som i övrigt finns i informationssystemet. Befogenheten möjliggör att den interna trafiken i datasystem granskas. Sådan intern trafik är till exempel tekniskt utbyte av meddelanden mellan ett gränssnitt som används av en statlig aktör och en informationslagringsplattform i dess bakgrund och meddelandetrafik som administreras av en statlig aktör mellan olika användare av ett datasystem. Spaning på den tekniska kontrolltrafiken mellan ett datasystems komponenter ger även möjlighet till att ta fram en övergripande bild av datasystemets interna funktion, de uppgifter som de innehåller och det hot som de bildar. Föremålet för befogenheten kan vara till exempel en terminalutrustning, ett användargränssnitt och en kommunikationsprogramvara som används i teleterminalutrustningen, terminalutrustningens datatrafiksförbindelse och de routrar, servrar och lagringstjänster (molntjänster) som används av en statlig aktör, till den del som en statlig aktör administrerar dessa.

Vid underrättelseinhämtning i Finland som avser statliga aktörers datasystem kombineras till vissa delar de nuvarande befogenheterna. Till exempel i fråga om data som lagrats i en

anordning och en programvara handlar det om en åtgärd som liknar teknisk observation av utrustning och då informationen rör sig från terminalutrustningen till en molntjänst handlar det om en åtgärd som liknar teleavlyssning, om information inhämtas exempelvis från ett datasystems router som ansluts till ett allmänt kommunikationsnät.

I princip innehas rätten att använda ett datasystem som administreras av en statlig aktör endast av dem till vilka den statliga aktören beviljat sådan rätt. Således riktar sig inte underrättelseinhämtning som avser datasystem till en slumpmässig grupp av personer, utan till dem till vilka en statlig aktör beviljat behörighet, såsom dess arbetstagare.

Föremålet för befogenheten är inte heller ett externt datasystem, såsom en plattform inom sociala medier, utan ett datasystem som uttryckligen är i den statliga aktörens egen användning och användningen av det. Dock är det via ett datasystem som administreras av en statlig aktör möjligt att exempelvis via en tjänst inom sociala medier producera information, från vilken det är möjligt att inhämta information till den del som den produceras i en statlig aktörs datasystem. När informationen har levererats till en tjänst inom sociala medier, ska informationen skaffas med en annan lämplig metod för underrättelseinhämtning än underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem, då det inte längre i fråga om plattformen för sociala medier handlar om en statlig aktörs datasystem. Även bestämmelserna om principerna i lagen styr till detta.

I paragrafens 1 mom. föreskrivs att man med i paragrafen avsedd underrättelseinhämtning som avser en statlig aktörs datasystem i Finland avser att information inhämtas från en del av ett datasystem som en statlig aktör administrerar eller använder i det finska territoriet, om delen genomför eller främjar den verksamhet som är föremål för ett underrättelseuppdrag eller lagrar eller förmedlar information som hänför sig till den verksamhet som är föremål för ett underrättelseuppdrag. Bestämmelsen begränsar den i paragrafen avsedda underrättelseinhämtning som avser datatrafik att täcka de delar av ett datasystem vilka finns i Finland. Med administrering avses att en statlig aktör har rätt att använda en viss anordning eller programvara och aktören kan besluta om användningen av anordningen eller programvaran inom ramen för behörigheten. Till exempel i fråga om information som lagras i en molntjänst omfattar administreringen del i vilken en statlig aktör kan lagra uppgifter, inte hela molntjänsten.

Användningen täcker även situationer där till exempel en statsattribuerad APT-aktör kapat en del av ett datasystem för eget bruk och vidtar skadliga cyberåtgärder i den kapade delen av datasystemet. Till denna del hänför sig och avgränsar sig användningen av metoden endast till den del av datasystemet vilken brutits eller som i övrigt används av APT-aktören och den statliga aktörens verksamhet i anknytning till detta. Överskottsinformation utplånas enligt bestämmelserna om utplåning och med hänsyn till underrättelseförbuden. Redan vid förberedelserna av användningen av befogenheten beaktas hur man undviker att upptäcka överskottsinformation och hur man säkerställer att överskottsinformation utplånas effektivt, om sådan på ett oförutsett blir föremål för underrättelseinhämtning.

I fråga om befogenheten ska man även beakta definitionen av en statlig aktör, som även täcker aktörer som förfar under styrning av en statlig aktör. En proxyaktör för en statlig aktör kan använda en del av ett datasystem och styrd av den statliga aktören vidta skadliga åtgärder mot Finlands försvar eller den nationella säkerheten.

I paragrafen avsedd underrättelseinhämtning som avser datatrafik hänför sig tekniskt sett till den logiska helhet som bildas av anordningar och virtuella system som kommunicerar sinsemellan i ett visst syfte som utgör ett allvarligt militärt hot eller som hotar den nationella

säkerheten, varvid inget tillstånd förutsätts separat för varje sådan anordning eller programvara som hör till helheten eller en datatrafikförbindelse som kopplar samman anordningar.

I paragrafen avsedd underrättelseinhämtning som avser datasystem handlar inte om underrättelseinhämtning som gäller enskilda personer eller anordningar, utan ett datasystem är ofta en föränderlig helhet. På grund av detta kan föremålet för underrättelseinhämtning även vara en statlig aktörs nya anordningar och användare, som inte utgjort en del av datasystemet eller användningen av det då underrättelseinhämtningen började. Naturligtvis kan personer och anordningar bli föremål för användning av metoden för underrättelseinhämtning endast till den del som de tekniskt sett anknyter till datasystemet. Om avsikten är att få uppgifter även till andra delar från teleterminalutrustningen för en systemanvändare, handlar det om användning av en annan metod för underrättelseinhämtning.

Information kan inhämtas antingen från hela datasystemet eller från en viss logisk eller fysisk del av ett datasystem, vilken genomför någon funktionalitet i datasystemet eller som i övrigt kan fastställas som en separat del av datasystemet baserat på datasystemets användare eller på uppgiftsinnehåll som på befogade grunder finns i en del av datasystemet. Inhämtande av information kan riktas till exempel på:

- 1) datanätinfrastruktur som en cyberhopsaktör byggt upp och använder, inbegripet de servrar, kapade anordningar och datatrafikförbindelser som hör till den,
- 2) ett visst användarkonto i en fildelningstjänst,
- 3) en kommunikationstjänst som används av en viss persongrupp eller organisation,
- 4) uppgifter om en teleterminalutrustning, vilka den lagrat i en molntjänst via olika applikationer,
- 5) en tjänst som administreras på virtualiserat sätt av en tjänsteleverantör och dess uppgiftsinnehåll, men inte annat uppgiftsinnehåll i samma fysiska server, vilket innehas av andra aktörer,
- 6) abstrakta informationsresurser, såsom vissa transaktioner av virtuella valutor.

Befogenheten möjliggör att militärunderrättelsemyndigheten på ett mer föregripande sätt än tidigare genomför underrättelseinhämtning som avser datasystem och identifierar hot. Detta möjliggör att militärunderrättelsemyndigheten i identifierade datasystem kan leta efter en sådan information som är avsedd att inhämtas och identifiera nya datasystem som är en del av militär verksamhet eller verksamhet som orsakar ett allvarligt hot för den nationella säkerheten.

Inhämtrandet av information från ett meddelande som inkommer eller avgår från ett datasystem möjliggör å sin sida underrättelseinhämtning som avser datasystemets drift i förhållande till dess cybermiljö, det vill säga till exempel hur datasystemet utför kommandon som ges av en cyberhopsaktör eller hurudant hot det i övrigt bildar.

Datasystemhelheten avgränsas exempelvis utifrån kommunikationen mellan de anordningar som utgör föremål och behörigheterna. Anordningarna i helheten kommunicerar med andra anordningar som hör till och används i datasystemhelheten och programvarorna har behörigheter till vissa anordningar och andra programvaror. Till exempel är det utifrån dessa uppgifter och de inhämtade uppgifterna även möjligt att till exempel från en datacentrals server avgränsa ett lagringsutrymme eller serverskåp som hör till datasystemhelheten och som används i datasystemet. Underrättelseinhämtning som avser datasystem förutsätter inte genomgång av omfattande datatrafikflöden eller datamassor som inte definierats i förväg, varför verksamheten således inte handlar om verksamhet som motsvarar underrättelseinhämtning som avser datatrafik, där inhämtrandet av information baserar sig på användning av sökbegrepp som beskriver föremålet.

Det står klart att underrättelseinhämtning som avser datasystem inte hänför sig till information i datacentralen, såsom uppgifter som inte definierats i förväg och som lagrats av enskilda personer. Användningen av befogenheten hänför sig inte på ett sätt som inte definierats i förväg till all potentiell information, utan den avgränsar sig till de delar som den statliga aktören använder enligt datasystemets infrastruktur. I det enklaste formen kan uppgifter i ett datasystem behandlas i en omfattning som helt motsvarar vad en enskild användare av datasystemet har möjlighet till. Således är det till exempel i fråga om en molntjänst inte möjligt att granska andra uppgifter än de som en enskild användare kan granska och behandla.

Eftersom datamängderna kan vara stora, kan uppgifterna naturligtvis behandlas automatiserat och manuellt, såsom annan information.

Principen om respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna styr till att inhämtandet av information ska riktas noggrant till en statlig aktörs information och datalager. Om det är oklart om inhämtandet av information hänför sig till ett datalager som i regel innehåller uppgifter om enskilda personer, har militärunderrättelsemyndigheten en accentuerade utrednings- och motiveringsskyldighet.

Paragrafens 2 mom. innehåller en begränsning av underrättelseinhämtning som avser datasystem. Eftersom datasystem kan handla om en helhet av anordningar och programvaror som även är omfattande, kan underrättelseinhämtning som avser datasystem användas endast i den omfattning som är nödvändig med tanke på den verksamhet som är föremål för underrättelseuppdraget. Med andra ord är det möjligt att från den första upptäckta punkten i ett datasystem övergå även till andra anordningar och programvaror i datasystemet, om de anknyter till underrättelseuppdraget och datasystemhelheten. Å andra sidan är det inte tillåtet att inhämta information från övriga delar av ett datasystem, eftersom det utvidgar inhämtandet av information till annat än vad som är nödvändigt.

I paragrafen om beslutsfattande föreslås separata bestämmelser om beslutsfattandet om fogande av en ny teleterminalutrustning, teleadress, anordning eller programvara. Eftersom ett separat beslut fattas om fogandet, kan underrättelsetillsynsombudsmannen övervaka verksamheten effektivt.

Det står klart att andra uppgifter i ett informationssystem än de som gäller en statlig aktör som utgör objektet för underrättelseuppdraget inte får inhämtas. Om sådana uppgifter blir föremål för metoden för underrättelseinhämtning, ska de utplånas enligt bestämmelserna om utplåning. I propositionen föreslås dessutom att 85 § i lagen ändras, då underrättelseinhämtning som avser datasystem enligt bestämmelsen ska avbrytas, om den är fel inriktad. Befogenheten omfattas även av protokollföringsskyldigheten och skyldigheten att granska upptagningar och handlingar på samma sätt som för uppgifter som inhämtats med andra metoder för underrättelseinhämtning.

Utvövningen av befogenheten begränsas även av förbuden mot underrättelseinhämtning och observations- och avlyssningsförbuden samt de allmänna principerna i lagen.

61 b §. *Beslut om underrättelseinhämtning i hemlandet som avser statliga aktörers datasystem.* Paragrafen innehåller bestämmelser om beslutsfattandet. Beslutsfattandet motsvarar de metoder för underrättelseinhämtning som tekniskt sett kombineras vid underrättelseinhämtning som avser datatrafik, det vill säga till exempel teleavlyssning och teleövervakning.

Enligt paragrafens 1 mom. ska ett yrkande till domstol göras av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Enligt paragrafens 2 mom. är ett tillstånd giltigt i högst sex månader åt gången.

Paragrafens 3 mom. innehåller bestämmelser om de fakta som ska nämnas i ett yrkande och i ett beslut. I 1 punkten i momentet avses med det underrättelseuppdrag som ligger till grund för åtgärden ett underrättelseuppdrag enligt 10 § 6 punkten. På samma sätt som för de andra metoderna för underrättelseinhämtning ska ett underrättelseuppdrag ligga till grund för användningen av en metod för underrättelseinhämtning. Yrkandet och beslutet ska redogöra för målet med åtgärden, vilket man strävar efter att uppnå genom användningen av metoden för underrättelseinhämtning. Målet för användningen av befogenheten ska fastställas med tillräcklig precision.

Enligt 2 punkten i momentet ska man i ett yrkande och ett beslut fastställa den statliga aktör som är föremål för åtgärden och det datasystem som den använder. I enlighet med definitionen ska den statliga aktören kunna namnges. Det kan handla om en statlig myndighet som opererar på finskt territorium eller en aktör som styrs av och lyder under en sådan. I varje fall ska den statliga kopplingen föras fram och motiveras.

I enlighet med punkten ska man i yrkandet så noggrant som möjligt fastställa systemhelheten på så sätt att en domstol har möjlighet att entydigt förstå och övervaka mot hurudan datasystemhelhet och vems hanteringsrätt eller användning verksamheten riktar sig mot.

Beskrivningen av systemet kan ske till exempel genom att beskriva den logiska helheten i det datasystem som utgör objekt. Med logisk helhet avses en abstrakt och teknikneutral beskrivning av hur delarna i informationssystemet fungerar tillsammans. Den logiska helheten redogör inte för med vilka anordningar eller programmeringsspråk systemet har genomförts, utan hur informationen rör sig, vilka funktionaliteter systemet erbjuder och hur de olika delar är sammankopplade. Datasystemets logiska nivå svarar på frågan om hur systemets funktionalitet har ordnats utan fysiska detaljer. Inom ramen för den logiska helhet som definierats i tillståndet är det möjligt att rikta underrättelseinhämtning som avser datasystem mot anordningar, programvaror och dataöverföringskanaler.

Ofta kan en militärunderrättelsemyndighet känna till exempelvis en anordning som hänför sig till den logiska helheten i ett informationssystem. Denna anordning ska anges i det krav som framförs till domstolen. Via en känd anordning fås information om datasystemet och utifrån de inhämtade uppgifterna fås en bättre bild av datasystemet och på så sätt är det möjligt att inhämta information från systemet övriga delar och via dessa.

Befogenheten handlar inte om anordningar eller teleadresser som används av en enskild person, utan om en helhet med delar som fysiskt eller logiskt är kopplade till varandra. På grund av detta ska man fastställa det datasystem som används med tillräcklig precision i ett yrkande och tillstånd. Det kan handla om exempelvis ett ärendehanteringssystem, där de uppgifter som matas in i systemet av en användare syns på anordningens skärm, men lagringen sker i en molntjänst.

Befogenheten täcker även de nya användare, anordningar och utrustningar som blir en del av eller förenas med datasystemet. På grund av detta är det inte möjligt att i ett yrkande eller ett tillstånd fastställa ett datasystem enligt anordning eller teleadress.

Momentets 3 punkt är centralt med tanke på beslutsfattandet. I ett yrkande och beslut ska man inkludera de fakta som ligger till grund för förutsättningarna för och inriktningen av underrättelseinhämtning som avser ett inhemskt datasystem. 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 metod för underrättelseinhämtning uppfylls.

De nämnda förutsättningarna handlar om de allmänna förutsättningarna för metoder för underrättelseinhämtning enligt 12 § och de förutsättningar som nämns i 61 a §, som gäller befogenheten. I ett yrkande och ett beslut ska man dessutom lägga fram tillräckliga fakta om underrättelseuppdraget och den statliga aktör som är föremål för den militära underrättelseverksamheten enligt 4 § i lagen och som ligger till grund för uppdraget.

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 i fråga om innehåll. 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. Trots ärendenas höga sekretessgrad kan domstolens prövning basera sig endast på att sökanden berättar öppet och med rätt innehåll för domstolen om den verksamhet som är föremål för inhämtandet av information genom att använda metoder för underrättelseinhämtning och om objektet.

Enligt 4 punkten i momentet ska giltighetstiden med angivande av klockslag inkluderas i ett yrkande och ett beslut.

Enligt 5 punkten i momentet ska man i ett yrkande och ett beslut nämna den tjänsteman som leder och övervakar underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem.

Enligt 6 punkten i momentet ska man inkludera eventuella begränsningar och villkor i ett yrkande eller ett beslut. En domstol kan i sitt beslut ställa begränsningar och villkor för användning av en metod för underrättelseinhämtning. Om sådana begränsningar och villkor är kända redan då ett yrkande utarbetas, ska den som framställer yrkandet överväga att skriva in dem redan i själva yrkandet.

62 §. Underrättelseinhämtning som avser utländska datasystem. Paragrafens 2 mom. ändras. I och med ändringen får befogenheten utövas även av andra militärunderrättelsemyndigheter än Försvarsmaktens underrättelsetjänst. I och med att den militära underrättelseverksamheten har utvecklats har man observerat ett behov av att militärunderrättelsemyndigheten allmänt har ett behov av använda underrättelseinhämtning som avser utländska datasystem.

Ett nytt 4 mom. fogas till paragrafen. Enligt det kan en militärunderrättelsemyndighet vidta behövliga datatekniska åtgärder i ett datasystem utanför det finländska territoriet, om man med eller via datasystemet orsakar ett allvarligt hot för Finlands landsförsvar eller den nationella säkerheten. De datatekniska åtgärderna kan gälla till exempel åtgärder för att försöka hindra systemets funktion helt eller delvis eller störa användningen av informationssystemet.

Med åtgärderna avses datatekniska metoder, varför det inte är möjligt att vidta fysiska åtgärder för kinetisk påverkan med stöd av bestämmelsen. Det bör observeras att man genom ett datasystem kan genomföra åtgärder som äger rum i den fysiska världen, såsom i fallet för ett system för funktionsstyrning.

I enlighet med lagens tillämpningsområde och regleringen kring underrättelseinhämtning som avser datasystem utomlands är användningsområdet för bestämmelsen bundet till militär underrättelseverksamhet, varför det inte är möjligt att vidta endast förhindrande åtgärder med stöd av bestämmelsen. I praktiken är en förutsättning för att använda bestämmelsen således att det i första hand handlar om underrättelseinhämtning. I praktiken kan denna situation bli aktuell exempelvis om föremålet för underrättelseinhämtning är ett datasystem som sedermera används för sådan allvarlig hotande verksamhet som beskrivits i bestämmelsen eller för att möjliggöra sådan. Befogenheten kan även utövas vid tecken på verksamhet som allvarligt äventyrar Finlands försvar eller den nationella säkerheten, vilken leder till att en underrättelseoperation inleds, varvid det är möjligt att vid behov rikta de åtgärder som avses i bestämmelsen på det datasystem som orsakar färan.

Åtgärderna kan bedömas rikta sig noggrant i praktiken alltid då det datasystem som utgör föremål redan är föremål för militär underrättelseinhämtning.

Eftersom det handlar om åtgärder som vidtas inom en annan stats territorium, ska man i bedömningen av åtgärden beakta den internationella rätten och de randvillkor som den ställer. Den internationella rätten i cybermiljön har behandlats i den allmänna motiveringen i denna proposition.

Med proportionalitet enligt bestämmelsen avses att åtgärden ska riktas noggrant mot verksamhet som utgör ett allvarligt hot, och med den får man inte orsaka större skada eller olägenhet än vad som är nödvändigt för att kunna vidta åtgärden. Innan åtgärden vidtas ska även en noggrann bedömning av dess konsekvenser göras.

Åtgärdernas konsekvenser ska även vara temporära och de ska avslutas direkt då det hotet har avvärijts.

Med nödvändighet enligt bestämmelsen avses att verksamhet som utgör ett hot inte kan hindras eller avslutas med andra metoder eller att användning av andra metoder förutsätter att avsevärda resurser används. Så som tidigare lagts fram i denna proposition, anser Finland att den internationella rätten är fullständigt tillämplig i cybermiljön. Således ska nödvändigheten bedömas även i den internationella rättens kontext och i första hand ska man bedöma möjligheten att använda andra metoder, såsom diplomati och retorsion. Det är möjligt att reagera på fientlig verksamhet även genom att begära att en annan stats CERT-enhet ingriper i verksamhet i den stats territorium. I sista hand kan det handla om att åberopa en i statsansvarsregleringen avsedd nödvändighet enligt den internationella rätten (så kallad plea of necessity).

Det bör även observeras att enligt den internationella rätten har en stat rätt att skydda sig mot oerättigad verksamhet och suveränitetskränkningar kan besvaras med de metoder som den internationella rätten medger. Det är ändamålsenligt att varje självständiga stat har tillgång till ett mångsidigt utbud av metoder för att förbereda sig och svara på olika hot mot staten såväl i normala förhållanden som i undantagsförhållanden. En sådan helhet stärker statens förmåga att skydda sin suveränitet, upprätthålla de vitala samhällsfunktionerna och att i rätt tid och på ett proportionellt sätt reagera på situationer som kan underminera dess säkerhet eller funktionsförmåga.

Eftersom de uppgifter som avses i bestämmelsen i vissa situationer kan leda till utrikes- och säkerhetspolitiska konsekvenser som till och med kan vara signifikativa, ska åtgärderna behandlas i det förfarande som avses i lagens 15 §. Åtgärderna förutsätter även behandling för att förbereda ett gemensamt möte för utrikes- och säkerhetspolitiska ministerutskottet och

republikens president. Även om det operativa beslutet fattas av huvudstabens underrättelsechef, ska det utrikes- och säkerhetspolitiska beslutet fattas innan dess.

Det står klart att de åtgärder som avses i momentet inte får överskrida tröskeln för väpnat våld enligt den internationella rätten och befogenheten får utövas endast för att förhindra och störa användning av ett datasystem som orsakar ett allvarligt hot för Finlands landsförsvar eller den nationella säkerheten.

APT-aktörer är ett vanligt exempel på verksamhet som orsakar ett allvarligt hot för landsförsvaret och den nationella säkerheten. APT-aktörerna (Advanced Persistent Threat) är cyberhofsgrupper som arbetar under en lång tid, på ett obemärkt sätt och med statsstöd och riktar attacker mot objekt som är viktiga för samhället, såsom förvaltningen, kritisk infrastruktur och företag. De agerar synnerligen systematiskt: de gör intrång, håller sig gömda och stjälar information eller stör verksamheten på lång sikt. Flera APT-aktörer har redan attribuerats till en viss stat.

APT-aktörerna måste bygga upp en infrastruktur för sin verksamhet (till exempel servrar, datatrafikförbindelser och informationssystem), som genomförs utan att den egentliga ägaren eller innehavaren är medveten om det till exempel genom att dra nytta av sabotageprogram och sårbarheter. För att genomföra den egentliga cyberattacken, styrs infrastrukturen från kommandoservrar.

Militärunderrättelsemyndigheterna kan redan för närvarande bevaka APT-aktörer med stöd av sin befogenhet, men deras verksamhet kan endast bevakas och information som fås genom bevakningen kan överlätas till andra myndigheter. Följderna av APT-aktörernas verksamhet kan förebyggas på finskt territorium, men detta hindrar inte egentlig verksamhet och bekämpningsåtgärderna orsakar kostnader.

Bestämmelsen möjliggör inte att militärunderrättelsemyndigheten vidtar attackåtgärder. Med stöd av bestämmelsen är det inte möjligt att vidta exempelvis destruktiva åtgärder mot en viss stats kritiska infrastruktur, så att funktionen i en viss stats samhälle störs.

Även om man anser att bestämmelsen inte handlar om inhämtande av information enligt 3 § i lagen, är det i enlighet med de synpunkter som gäller ändamålsenligheten befoget att utfärda bestämmelser om en möjlighet att agera i samband med befogenheten att inhämta information. I situationer enligt bestämmelsen finns militärunderrättelsemyndigheten redan vid objektet och militärunderrättelsemyndigheten har möjlighet att agera i de situationer som avses i bestämmelsen.

En militärunderrättelsemyndighet är den enda myndighet som har behörighet och befogenhet att inhämta information från datasystem som finns utomlands. Som en del av Försvarsmakten har en militärunderrättelsemyndighet dessutom kunskande inom tryggheten av rikets territoriella integritet och den anknutna strategiska, operativa och taktiska planeringen.

63 §. Beslut om underrättelseinhämtning som avser utländska datasystem. Ett nytt 3 mom. fogas till paragrafen, varvid det nuvarande 3 mom. blir nya 4 mom. Paragrafen innehåller bestämmelser om beslutsfattande som gäller 62 § 4 mom.

Utöver de utrikes- och säkerhetspolitiska aspekterna ska man i det utrikes- och säkerhetspolitiskt känsliga området alltid beakta även den nationella lagstiftningen och den internationella rätten i beslutsfattandet om en åtgärd. Ovan avsedda ståndpunkter ska beredas

tväradministrativt i förfarandet enligt 15 § i lagen. Beslutet ska även behandlas på förberedande sätt i utrikes- och säkerhetspolitiska ministerutskottet.

Vid beslut om användning av befogenheten enligt föreslagna 62 § 4 mom. ska man alltid beakta åtgärdens proportionalitet, inbegripet konsekvenserna för objektet, risken för eventuell eskalering samt potentiella motåtgärder mot Finland och deras konsekvenser.

Även operationssäkerheten är en central del av konsekvensbedömningen av åtgärderna. Om en åtgärd inte kan vidtas på ett operativt säkert sätt, ska den inte vidtas. I beslutsfattandet ska man alltid beakta de resurser som åtgärden kräver och sätta dem i proportion till de realistiska förväntade fördelarna.

I enlighet med momentet fattas beslutet av huvudstabens underrättelsechef. Beslutet förutsätter även att ärendet behandlas på förberedande enligt 15 § 2 mom. i lagen och i utrikes- och säkerhetspolitiska ministerutskottet. Det exekutiva beslutet om operationen enligt beslutet fattas av den instans som ansvarar för den operativa verksamheten efter detta, det vill säga militärunderrättelsemyndigheten. Förfarandet kan anses vara ändamålsenligt även på grund av den utrikespolitiskt känsliga karaktären.

Enligt föreslagna 62 § 4 mom. förutsätter vidtagandet av åtgärderna en exakt operativ och politisk bedömning. Med tanke på beslutsfattandet är det centralt att fastställa föremålet för åtgärden, det vill säga datasystem mot vilket åtgärder riktas (en anordning för databehandling, en anordning för dataöverföring och en interoperativ helhet av programvaror som behandlar data). Utgångspunkten är att militärunderrättelsemyndigheten redan har en exakt bild av det datasystem som utgör föremål.

Det är även centralt att bedöma det hot som orsakas av informationssystemet eller via det. De funktioner som har definierats i 4 § i lagen ses som ett allvarligt hot. I bedömningen ska man rikta uppmärksamhet på hur snabbt hotet kan bli verklighet. Om en annan stat vill rikta skadliga åtgärder mot Finland, kräver detta förberedande åtgärder av den som vidtar åtgärden. Det centrala är att bedöma i vilket skede man med tillräckligt stor sannolikhet kan konstateras att åtgärderna kommer att rikta sig mot Finland. Detta kan konstateras till exempel då man i ett datasystem matar in uppgifter som gäller Finland eller föremål som finns i Finland.

Åtgärderna förutsätter även noggrann planering, om man vill uppnå det eftersträvande slutresultatet. Vidtagandet av åtgärder ska även övervakas såväl juridiskt som operativt.

Ovan beskrivna och andra synpunkter ska bedömas i ett förfarande enligt 15 § i lagen och i utrikes- och säkerhetspolitiska ministerutskottet, som kan uttrycka sin egen uppfattning om dessa.

64 §. Militär underrättelseinhämtning utomlands. Till paragrafens 1 mom. fogas en hänvisning till 51 § om användning av informationskällor och dess 3 mom. I och med tillägget behöver man inte iaktta förbudet mot att inhämta information med myndighetsbefogenheter vid användning av informationskällor utomlands.

På grund av de gällande bestämmelserna har oklarhet orsakats av huruvida förbudet att utöva myndighetsbefogenheter handlar om befogenheter för finska myndigheter eller för myndigheterna i målstaten. I vissa stater kan myndigheternas befogenheter vara synnerligen omfattande, varför det kan förbli oklart om informationskällan utövar myndighetsbefogenheter eller inte.

I och med den nya hänvisningen ska det vid avvikelse dock handla om nödvändighet.

Paragrafens 2 mom. delas upp i två moment. I och med den nya formuleringen gäller 2 mom. beslutsfattande och 3 mom. samtycke av en tjänsteman.

Enligt paragrafens 2 mom. beslutar huvudstabens underrättelsechef om militär underrättelseinhämtning utomlands och om de metoder för underrättelseinhämtning som är tillåtna där. Utifrån den gällande bestämmelsen har det varit oklart om huvudstabens underrättelsechef bestämmer även om användning av enskilda metoder för underrättelseinhämtning. Detta kan ha skapat ett problem i praktiken vid genomförande av underrättelseoperationer utomlands, och ett beslut av huvudstabens underrättelsechef förutsätts för att använda en enskild metod för underrättelseinhämtning.

I och med den föreslagna ändringen fattar huvudstabens underrättelsechef ett beslut om militär underrättelseinhämtning utomlands (en underrättelseoperation) och de metoder för underrättelseinhämtning som används i den, det vill säga vilka metoder för underrättelseinhämtning som är tillåtna i den aktuella operationen. Beslutet om användning av en metod för underrättelseinhämtning enligt beslutet kan göras av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman, som arbetar närmare verksamheten i praktiken. Ändringen förtydligar rättsläget och tjänstemannens rättsskydd förbättras.

På grund av den utrikespolitiska känsligheten i anknytning till underrättelseinhämtning utomlands ska man beakta prioriteringarna i underrättelseinhämtningen och regleringen i 15 § och eventuella riktlinjer som mottagits via dessa.

Paragrafens nya 3 mom. innehåller bestämmelser om samtycke av en tjänsteman vid en militärunderrättelsemyndighet, vilken deltar i militär underrättelseinhämtning utomlands. Bestämmelsen motsvarar nuläget, som har föreskrivits med riksdagens medverkan. Ett samtycke är fortfarande alltid en förutsättning för att åka utomlands.

I och med de föreslagna ändringarna övergår den gällande paragrafens 3 mom. till att bli nya 4 mom.

66 §. *Behandling av tekniska data för identifiering av en del av ett kommunikationsnät och för identifiering av dirigeringen av och ändringar i datatrafiken.* Det föreslås att paragrafen innehåller bestämmelser om behandling av tekniska data enligt den gällande lagen, men därtill även om behandling av tekniska data för att identifiera dirigeringen av och ändringar i datatrafiken. På grund av detta ändras även paragrafens rubrik för att innehållsmässigt överensstämma med den nya formuleringen av paragrafen.

I 1 mom. i gällande 66 § har behandlingen av tekniska data bundits till kortvarighet, som i praktiken ansetts vara svårt att genomföra och inte heller ansetts vara ändamålsenligt. Den information som fås med stöd av befogenheten är i enlighet med 10 § 11 punkten i lagen uppgifter om datatrafiken som gäller andra uppgifter än uppgifter om innehållet i ett meddelande. Dessa uppgifter kan vara bland annat IP-adressrymder, olika protokoll och anordningsnummer. Även om till exempel en IP-adress i sig kan identifiera en enskild person, är det med stöd av befogenheten inte möjligt att närmare utreda användaren av en IP-adress eller dennes kommunikation och uppgifterna kan inte användas för ett annat syfte än för teknisk analys. Även om den inhämtade informationen i sig är en personuppgift, är det med stöd av befogenheten inte möjligt att förena personuppgiften med en enskild fysisk person eller

organisation. På grund av detta kan slopandet av den tillfälliga karaktären inte anses leda till att behandlingen av tekniska data utgör så kallad massaövervakning.

Vid utövning av den befogenhet som avses i paragrafen är det vid behov möjligt att använda även sökbegrepp som hänför sig till datatrafik, så att den mängd information som fås kan avgränsas till vad som är maximalt väsentligt redan i initialskedet. Syftet med befogenheten är att identifiera de väsentliga delarna av ett kommunikationsnät, varför data med tanke på behandlingen av tekniska data avgränsas väsentligt till exempel med IP-adressrymden för ett visst geografiskt område. Det finns dock inte något behov av att utfärda separata bestämmelser om detta på grund av befogenhetens art.

Även om hänvisningen till tillfällig karaktär stryks från paragrafen och man föreslår ett nytt användningsändamål för behandling av tekniska data om datatrafik i paragrafen, är verksamheten fortfarande noggrant övervakad såväl internt som externt. Underrättelsetillsynsombudsmannens roll är accentuerad i den externa övervakningen.

Från paragrafen stryks även en analys som gjorts med hjälp av automatisk behandling av uppgifterna. Det nämnda kan anses vara onödigt eftersom en analys i praktiken alltid görs genom automatisk behandling av data. Å andra sidan är det möjligt att det uppkommer situationer där det är nödvändigt att göra analysen eller att anrika den manuellt. I varje fall är de uppgifter som används tekniska data om datatrafik och de bakomliggande personerna kan inte utredas genom att behandla tekniska data.

I 1 punkten i paragrafens 1 mom. regleras behandlingen av tekniska data för att identifiera en del av ett kommunikationsnät. I praktiken motsvarar punkten bestämmelsen i 66 § 1 mom. i den gällande lagen. Med behandling av tekniska data avses behandling av tekniska data om datatrafik för att utöva befogenheterna till underrättelseinhämtning som avser datatrafik enligt 68 och 70 § i syfte att identifiera väsentliga delar av ett kommunikationsnät. Målet med befogenheten är att identifiera de delar av ett kommunikationsnät som överskrider Finlands gräns, såsom fibrer och fibrernas våglängder, via vilken datatrafiken för en aktör som är föremål för militär underrättelseinhämtning går. Med befogenheten är det inte möjligt att inhämta annan data än tekniska data om datatrafik och endast för att producera en analys i syfte att identifiera en del av ett kommunikationsnät. Det är inte möjligt att använda innehållsuppgifterna i ett meddelande.

Paragrafens 1 mom. 2 punkten är ny. Utifrån punkten kan tekniska data om datatrafik följas och analyseras för att utreda om datatrafiken dirigeras på ett nytt sätt eller om allmänna förändringar skett i datatrafiken. Genom befogenheten är det möjligt att upptäcka förändringar som anknyter till ett fysiskt kommunikationsnät, såsom en uppgång i den tekniska kapaciteten i en del av ett kommunikationsnät, samt förändringar på den logiska nivån för datatrafiken.

En central egenskap i datatrafik och i synnerhet i funktionen för ett nät som är uppkopplat till internet är att informationen går maximalt effektivt från avsändaren till mottagaren. På grund av detta delas till exempel ett enskilt e-postmeddelande upp i flera datatrafikpaket, av vilka vart och ett går via den rutt som är effektivast för det enskilda paketet från avsändaren till mottagaren. Detta innebär att dirigeringen av datatrafiken för ett objekt för militär underrättelseinhämtning kan ändras väldigt snabbt. Med stöd av den nu behandlade bestämmelsen kan dirigeringen följas.

Med de ändringar i datatrafiken till vilka det hänvisas i bestämmelsen avses att man mer allmänt följer ändringar i datatrafiken och kommunikationsnätet med hjälp av tekniska data om datatrafiken. Tekniska ändringar kan ske i ett kommunikationsnät och nya anordningar tas i

bruk. Detta kan vara av betydelse för funktionen för ett system för underrättelseinhämtning som avser datatrafik och de anordningar tekniska installationer och justeringar som behövs vid underrättelseinhämtning som avser datatrafik. Utifrån de mottagna analyserna är det möjligt att till exempel effektivisera upphandlingarna av anordningar och rikta dessa på ett ändamålsenligt sätt samt att göra behövliga ändringar i systemet för underrättelseinhämtning som avser datatrafik.

Det föreslås att paragrafens 2 mom., på ett sätt som motsvarar den gällande lagen, innehåller bestämmelser om att man i behandlingen av tekniska data inte får bilda information som gör det möjligt att identifiera en enskild fysisk person. Bestämmelsen är informativ. Paragrafen i sig gäller behandling av tekniska data om datatrafik och ingen personbundenhet kan läsas ut av den. I lagens principbestämmelser regleras principen om ändamålsbundenheten och grundlagens 2 § 3 mom. förutsätter att det allmänna iakttar lagen noggrant. Om en analys produceras för att identifiera en enskild person, överträder myndigheten även utan bestämmelsen sina tjänsteplikter och gör sig sannolikt skyldig till ett brott.

Enligt paragrafens 3 mom. får tekniska data som behandlas i behandlingen av tekniska data lagras i 18 månader. Enligt bestämmelsen får mängden tekniska data som förs in inte överstiga fem procent av kapaciteten i den del av ett kommunikationsnät som överskrider Finlands gräns och som är föremål för datainsamlingen, det vill säga av den maximala mängd datatrafik som en del av ett kommunikationsnät tekniskt sett kan transportera. Till exempel om den tekniska kapaciteten i en del av ett kommunikationsnät är 100 per sekund, får 5 tekniska uppgifter per sekund lagras. I praktiken är tekniska data som lagras slumpmässiga tekniska data.

I bestämmelsen ges militärunderrättelsemyndigheterna även rätt att lagra insamlade tekniska data i högst 18 månader. Lagrade data raderas efter 18 månader från lagringstidpunkten med en sekunds precision.

Lagrade uppgifter kan användas till exempel till stöd för de analyser som avses i 1 mom. 1 och 2 punkten i paragrafen eller för att fastställa sökbegrepp i enlighet med föreslagna 67 a § samt i samband med de egentliga befogenheterna till underrättelseinhämtning som avser datatrafik, vilka föreskrivits i 68 och 70 §. För utövning av de befogenheter som avses i ovan hänvisade paragrafer i syfte att använda här avsedda behandlade data förutsätts naturligtvis ett behörigt domstolstillstånd, som föreskrivs i 67 b § samt i 69 och 71 §. Lagrade tekniska data om datatrafik får inte användas självständigt för att utföra ett underrättelseuppdrag, om ett behörigt tillstånd för detta inte mottagits.

Lagring och användning av tekniska data förutsätter ett datasystem och förfaranden som garanterar att lagrade uppgifter inte kan användas för något annat än det avsedda ändamålet eller utan behörigt domstolstillstånd. Detta förutsätter en noggrann åtkomsthantering och övervakning.

Paragrafens 4 mom. innehåller bestämmelser om utplåning av information som fåtts vid behandling av tekniska data för identifiering av en del av ett kommunikationsnät och för identifiering av dirigeringen av och ändringar i datatrafiken. Enligt bestämmelsen ska uppgifter utplånas inom 18 månader från att de lagrats. Det handlar uttryckligen om de tekniska data om datatrafiken, vilka har lagrats enligt paragrafens 3 mom., inte om de som är en del av en statistisk analys eller som nått den fortsatta behandlingen via metoderna för underrättelseinhämtning enligt föreslagna 67 a § eller 68 eller 70 §.

Det bör observeras att en militärunderrättelsemyndighet inte kan använda de här avsedda uppgifterna i något annat sammanhang, om inte en domstol beviljat tillstånd för en sådan

befogenhet med vilken de här avsedda uppgifterna får behandlas. Således kan en militärunderrättelsemyndighet inte utreda till exempel identiteten på användaren av förmedlingsuppgifter genom att använda 104 § i lagen om militär underrättelseverksamhet om inte förmedlingsuppgifterna fås genom egentlig underrättelseinhämtning som avser datatrafik (68 eller 70 § i lagen). En militärunderrättelsemyndighet kan alltså utreda identiteten på användaren av förmedlingsuppgifter genom 104 §, om förmedlingsuppgiften fås i samband med underrättelseinhämtning som riktats mot datatrafik utifrån sökbegreppen.

67 §. *Beslut om behandling av tekniska data för identifiering av en del av ett kommunikationsnät och för identifiering av dirigeringen av och ändringar i datatrafiken.* I paragrafen görs de ändringar som beror på de ovan föreslagna ändringarna i 66 §. Paragrafens rubrik innehåller i enlighet med 66 § en hänvisning till beslut för identifiering av en del av ett kommunikationsnät och dirigeringen av och ändringar i datatrafiken.

I paragrafens 1 mom. görs en teknisk ändring med anledning av de ändringar som föreslagits avseende 66 §. Momentet hänvisar till identifiering av en del av ett kommunikationsnät och dirigeringen av och ändringar i datatrafiken.

Dessutom ändras den tjänsteman som framför ett yrkande till domstolen från en tjänsteman från Försvarsmaktens underrättelsetjänst till en tjänsteman hos en militärunderrättelsemyndighet. På grund av militärunderrättelsemyndighetens organisation är det inte ändamålsenligt att den som framför ett yrkande ska vara en tjänsteman uttryckligen från Försvarsmaktens underrättelsetjänst, utan att den som framför ett yrkande även kan vara en tjänsteman från huvudstabens underrättelseavdelning. Fortfarande är det väsentligt att tjänstemannen är en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Giltighetstiden för ett tillstånd som föreskrivits i paragrafens 2 mom. är sex månader i stället för tidigare tre månader. Den utsatta tiden på tre månader har ansetts vara obefogat kort med beaktande av att man genom att utöva befogenheten inte skaffar annan data än teknisk data om datatrafik för att göra en teknisk analys. En utsatt tid på högst sex månader ligger även i linje med de utsatta tiderna för egentlig underrättelseinhämtning som avser datatrafik, vilka föreskrivs i 69 och 71 § i lagen.

Tillståndets giltighetstid börjar löpa från det datum då tillståndet getts eller från det datum då beslutet fattats.

Enligt bestämmelsen kan tillståndet gälla även tiden innan ovan konstaterade datum då tillståndet utfärdats eller beslutet fattades, vilken kan vara längre än sex månader. I behandlingen av tekniska data är det möjligt att använda lagrade tekniska data enligt föreslagna 66 § 3 mom.

I 3 mom. 1 punkten i paragrafen görs de ändringar som följer av de föreslagna ändringarna av 66 §. Utöver ett geografiskt område eller en domän enligt den gällande 1 punkten fogas till punkten ett objekt vars datatrafik följs i fråga om dirigeringen och ändringar. Med objekt avses en aktör som är föremål för militär underrättelseinhämtning och vars datatrafik är föremål för inhämtande av information när det gäller dirigeringen av och ändringar i den. Det kan förutsätta att avgränsande sökbegrepp används, så att tekniska förändringar i objektets datatrafik kan bevakas. Naturligtvis ska man i yrkandet redogöra för hur tekniska ändringar i objektets datatrafik bevakas och vilka uppgifter som är tillgängliga för att möjliggöra bevakningen.

Enligt 3 mom. 2 punkten i paragrafen ska man i ett yrkande och ett beslut nämna de delar från kommunikationsnätet från vilka uppgifter hämtas. Inga ändringar föreslås för punkten.

Enligt 3 punkten i 3 mom. ska man i ett yrkande och ett beslut nämna den med användningen av metoder för underrättelseinhämtning särskilt förtroigna tjänsteman som leder och övervakar behandlingen. Inga ändringar föreslås för punkten.

Enligt 3 mom. 4 punkten i paragrafen ska man i ett yrkande och ett beslut nämna planen för genomförandet av behandlingen. Upprättandet av en plan ska även tillämpas på ändringen av 1 punkten i momentet, det vill säga på bevakningen av dirigeringen av och ändringar i datatrafiken. Således ska man i planen redogöra för hur bevakningen exakt kommer att genomföras.

67 a §. *Underrättelseinhämtning som avser datatrafik för fastställande av sökbegrepp.* Paragrafen är ny. Paragrafen innehåller bestämmelser om fastställande av nya sökbegrepp som behövs för att underrättelseinhämtning som avser datatrafik ska vara så riktad som möjligt. Med termen hänvisar man till att målen för militär underrättelseverksamhet i sig förblir samma som i den gällande lagen, men att exempelvis den teknik och de kommunikationsmetoder som målen använder i ett kommunikationsnät kan förändras. I synnerhet i den rådande säkerhetspolitiska situationen har den tekniska utvecklingscykeln blivit snabbare och man strävar efter att införa ny teknik och nya metoder i en snabbare takt än tidigare. De aktörer som är föremål för militär underrättelseverksamhet ändrar konstant sin verksamhet och de utvecklar nya förfaringssätt.

Syftet med den nya befogenheten är att fastställa sökbegrepp med en tillräcklig förmåga att skilja åt datatrafik. I nuläget fastställs nya sökbegrepp i alla situationer i praktiken i samband med den egentliga underrättelseinhämtning som avser datatrafik, men om den aktör som utgör objekt byter den tekniska kommunikationsmetoden, kan mottagandet av information från objektet upphöra på överraskande sätt.

Användningen av befogenheten är bunden till nödvändighet. I enlighet med definitionen av nödvändighet ska fastställandet av sökbegrepp med andra ord i praktiken vara omöjlig med andra metoder, den ska kräva väsentligt mer resurser eller så fördröjer användning av andra metoder oskäligt underrättelseinhämtningen. Detta kan vara fallet till exempel i en situation där man på ett överraskande sätt genom de använda sökbegreppen inte längre lyckas inhämta information från datatrafiken för en aktör som utgör objekt, men dock vet att objektet fortfarande kommunicerar regelbundet. Således kan det förmodas att objektet tagit i bruk en ny kommunikationsmetod, varför sökbegrepp som hänför sig till den nya kommunikationsmetoden ska vara i användning. I situationen kan information dock inhämtas med andra metoder för underrättelseinhämtning, men till exempel användning av metoder för underrättelseinhämtning utomlands kan inte anses utgöra ett realistiskt alternativ redan på grund av skyddet av tjänstemännens liv och hälsa, för att inte tala om de resurser och den tid som ska användas för underrättelseoperationen.

Enligt 1 mom. i paragrafen kan Försvarsmaktens underrättelsetjänst samla in datatrafik och lagra sådan för att fastställa sökbegrepp som gäller objekt för militär underrättelseinhämtning. Den datatrafik som rör sig i en del av kommunikationsnätet är sporadisk, det vill säga att man i första hand inte strävar efter att rikta fastställandet av nya sökbegrepp mot en viss datatrafik. Slumpmässig datatrafik rör sig alltså i datatrafikflödet.

Vid fastställandet av sökbegrepp utgör byteflödet i datatrafiken målet, från vilket man strävar efter att fastställa nya sökbegrepp utifrån regelbundenheten eller de tekniska särdragen i anknytning till datatrafiken hos den aktör som utgör objekt. Vid utövning av befogenheten sätts

datatrafiken inte i sådan form utifrån vilken en analytiker kan läsa det egentliga semantiska meddelandet, utan målet i verksamheten är att fastställa vilken datatrafik det överhuvudtaget handlar om (det övergripande byteflödet inklusive alla protokollager). Detta kan kräva att datatrafiken granskas på bytenivå, oberoende av protokollstackets struktur.

Om analysförmågan avgränsas endast till redan kända omständigheter i rubriksdata i de lägre datatrafikskikten (såsom IP-adressen), försämras möjligheterna att få insikt om eller dra slutsatser om naturen på datatrafiken. I detta sammanhang finns det även skäl att förstå att man med naturen på datatrafiken inte avser det talade eller skrivna betydelseinnehållet i kommunikation mellan människor, utan om vad som överförs i datatrafiken, mellan vilka aktörer eller system och med vilka tekniska metoder och särdrag.

I fråga om trafik som inte identifierats i förväg finns det inte någon utgångsinformation om till exempel var i byteflödet ett visst protokollager börjar eller var det slutar. Utredningen av detta kräver undersökningsarbete på bytenivå i datatrafiken, till exempel för att upptäcka återkommande scheman i datatrafiken. I vissa fall kan detta även vara en förutsättning för att kunna identifiera om det handlar om föremålets trafik eller inte.

En annan viktig synvinkel är även en bedömning av identifieringen av datatrafiken: om det inte finns förmåga att granska datatrafiken i oförändrad (rå) form, föreligger inte nödvändigtvis förutsättningar att bedöma om en viss protokollidentifiering eller objektträff är rätt eller så kallad felaktigt positiv.

Så som beskrivits tidigare i denna regeringsproposition kan sökbegrepp utgöras av bland annat tekniska data om datatrafiken, vilka används av objektet, och olika protokoll, med vilka kommunikationen förmedlas från avsändaren till mottagaren. Till exempel vid utveckling av nya kommunikationsprogram utvecklas även nya protokoll på samma gång. Den ofta använda kommunikationsapplikationen WhatsApp använder en omarbetad version av XMPP-protokollet och för krypteringen används krypteringsprotokollet Signal Protocol, medan kommunikationsapplikationen Telegram använder det egna krypterings- och kommunikationsprotokollet MTProto. Dessa protokoll kan för närvarande utgöra sökbegrepp, men nya protokoll som används för ett motsvarande användningsändamål utvecklas konstant utan att det nödvändigtvis finns närmare information om dessa innan en stor grupp användare använder protokollet. I synnerhet statliga aktörer strävar efter att utveckla sin kommunikation på så sätt att den teknik som används inte kommer att användas av en stor grupp av användare.

Syftet med fastställande av sökbegrepp enligt momentet är att hitta till exempel ovan beskrivna nya protokoll och andra uppgifter som kan användas som sökbegrepp, med vilka underrättelseinhämtning som avser datatrafik kan riktas mot ett objekt för militär underrättelseinhämtning och endast till nödvändig information.

Med tanke på befogenheten är det inte av betydelse om datatrafiken är krypterad. Även krypterad datatrafik överförs i datatrafiken i form av bit- och byteflöde och genom att tolka återkommande scheman i dessa är det möjligt att fastställa nya sökbegrepp. Vid undersökning av byteflödet är målet att skapa relevanser, med vilka det är möjligt att upptäcka information som kan utnyttjas för underrättelseinhämtningen. Även om trafiken är krypterad, utesluter den inte att relevanser bildas.

Befogenheterna gäller inte meddelandets innehåll, det vill säga utredning av det semantiska betydelseinnehållet, utan information hämtas exempelvis utifrån de särdrag som kan observeras i den så kallade nyttolasten.

I fastställandet av sökbegrepp strävar man även efter att utifrån regelbundenheten och särdragen i datatrafiken identifiera exempelvis hur avsändaren och mottagaren syns exempelvis i ett nytt identifierat protokoll.

I och med att nya sökbegrepp fastställs är det möjligt att utveckla sökbegreppen till noggrannare begrepp och på så sätt är det även möjligt att i mindre grad ingripa i datatrafik som är onödig med tanke underrättelseinhämtningen och i dess innehåll. Dessutom kan det bedömas att underrättelseinhämtning som avser datatrafik är effektivare, eftersom det är möjligt att inhämta information om objektets datatrafik på ett ännu smidigare sätt.

Enligt paragrafens 2 mom. får uppgifter i ett meddelandes betydelseinnehåll inte utnyttjas då sökbegrepp fastställs. Genom bestämmelsen skyddas betydelseinnehållet i ett meddelande och befogenheten har inte heller i övrigt som syfte att det ska utredas. Genom befogenheten i bestämmelsen kan inte heller en viss persons verksamhet utredas. Såsom konstateras i 1 mom., handlar fastställande av sökbegrepp uttryckligen om fastställande av sökbegrepp som träffar underrättelseobjektets datatrafik, inte objektets kommunikation eller utredning av något annat, till exempel privatlivet. Vid utredning av kommunikation handlar det om att utöva den befogenhet som avses i 68 och 70 § i lagen.

Det faktum att datatrafik, på det sätt som lagts fram ovan i denna proposition, består av datatrafikpaket bidrar till att förhindra att man ingriper i betydelseinnehållet i ett meddelande. Således är det betydelsefulla innehållet i ett meddelande i ett enskilt paket ofta litet – i praktiken är det aldrig möjligt att utifrån ett enskilt datatrafikpaket utreda någon förnuftig språklig betydelse, om inte datatrafikpaketen slås samman med tillräckligt många andra datatrafikpaket som anknyter till samma kommunikationshändelse.

Även om de uppgifter som inhämtas i sig kan vara personuppgifter, kan enkom denna information inte anses utgöra något betydande ingrepp i en persons integritet. Till exempel en IP-adress begränsar en anordning som är ansluten till ett nät på internet till en viss anordning, men den berättar inte i sig ännu något alls om anordningens användare. På motsvarande sätt berättar protokollen eller gruppen av sådana i sig inte något om innehållet i kommunikationen eller om användaren av protokollen, utöver att användaren i fråga använder dessa protokoll. Det faktum att man vet att en viss aktör använder vissa protokoll i sin kommunikation, förutsätter redan annan underrättelseinformation än den information som uppkommer genom fastställandet av sökbegrepp.

I momentet föreskrivs därtill uttryckligen att fastställandet av sökbegrepp inte får generera information som beskriver meddelandets innehåll eller information utifrån vilken det är möjligt att dra slutsatser om en persons privatliv. Således får det av slutresultat inte framgå till exempel om något meddelande innehåller en bifogad fil eller vad meddelandets semantiska innehåll varit. Dessutom får slutresultaten inte redogöra för vem som kommunicerar med vem och när. Befogenheten handlar uttryckligen om att man kan identifiera tekniska attribut som anknyter till objektet och det tekniska ramverket för objektets datatrafik, till vilket de närmare uppgifterna fogas för att den egentliga underrättelseinhämtningen som avser datatrafik ska hänföra sig till det nödvändiga.

Paragrafens 3 mom. innehåller bestämmelser om mängden datatrafik som ska användas för att fastställa sökbegrepp. Fastställandet av sökbegrepp kan hänföra sig till en del av ett kommunikationsnät som överskrider Finlands gräns. Den mängd datatrafik som samlas in och mot vilken det är möjligt att rikta fastställandet av sökbegrepp, får inte överskrida fem procent av kapaciteten i den del av ett kommunikationsnät som utgör objekt. Kapacitet hänvisar till den tekniska maximikapaciteten i en del av ett kommunikationsnät. I fastställandet av sökbegrepp

är volymen på datatrafiken med andra ord begränsad fysiskt till en del av ett kommunikationsnät som överskrider Finlands gräns och tekniskt till en viss volym av den datatrafik som rör sig i en del av ett kommunikationsnät. Om den tekniska kapaciteten i en del av ett kommunikationsnät som överskrider Finlands gräns är 100 per sekund, är det möjligt att fastställa sökbegrepp från en del på 5 per sekund av datatrafiken.

I praktiken avgränsar de tekniska attribut för datasystemet vilka används i fastställandet av sökbegrepp inhämtningen av information till en viss datamängd per sekund, inte till en procentuell andel. Om kapaciteten i en del av ett kommunikationsnät som utgör objekt på ett överraskande sätt ökar, är således den tidigare fastställda datamängden, vilken alltså är lägre än fem procent, fortfarande föremål för befogenheten. Om den tekniska kapaciteten i en del av ett kommunikationsnät ökar, förutsätter detta i praktiken tekniska ändringsarbeten i kommunikationsnätet, vilket kan upptäckas under tiden för användningen av befogenheten.

Skillnaden till behandlingen av tekniska data enligt vad som föreskrivs ovan i 66 § är att tekniska data kan inhämtas och lagras från datatrafik i hela kommunikationsnätet. Den sammanlagda mängden data som lagras får inte överskrida fem procent av den tekniska kapaciteten i en del av ett kommunikationsnät som överskrider Finlands gräns.

Föremålet för befogenheten i fråga om det nu behandlade fastställandet av sökbegrepp får vara fem procent av den tekniska kapaciteten i en del av ett kommunikationsnät som överskrider Finlands gräns och de fem procent av den datatrafik som når behandlingen får även lagras. Det vill säga att om den tekniska kapaciteten i en del av ett kommunikationsnät är 100 per sekund, får nya sökbegrepp fastställas utifrån en datatrafikmängd som motsvarar 5 per sekund. Således kan datatrafik från en del av ett kommunikationsnät som utgör objekt i en mängd som motsvarar 5 per sekund nå lagringen, från vilken även nya sökbegrepp fastställts.

De uppgifter som inhämtas med stöd av befogenheterna är uppgifter som inte ingår i betydelseinnehållet i ett meddelande och med dessa är det således inte möjligt att avsevärt ingripa i skyddet för privatlivet. Utifrån de uppgifter som inhämtas är det inte möjligt att identifiera enskilda personer och genom att utöva befogenheten i bestämmelsen är det inte möjligt att förena dem på ett sätt som gör att en enskild person kan identifieras. Det ovan konstaterade skulle även redan strida mot principen om ändamålsbundenhet.

Paragrafens 4 mom. innehåller bestämmelser om lagringstiden för uppgifter som används för att fastställa sökbegrepp. Enligt bestämmelsen ska insamlad och lagrad datatrafik utplånas tolv månader efter den tidpunkt då den samlats in. Således utplånas den lagrade datatrafiken med en sekunds precision inom tolv månader för att den lagrats.

Avgränsningen av de uppgifter som lagras gäller naturligtvis inte fastställda sökbegrepp, utan fastställda sökbegrepp kan användas så länge som det genom dem är möjligt att inhämta information om objektet i egentlig underrättelseinhämtning som avser datatrafik.

När sökbegrepp fastställs har historikdata en betydande roll för sökbegreppets precision. Eventuella nya sökbegrepp som observerats i processen för att fastställa nya sökbegrepp och deras precision kan bedömas genom att jämföra dem med tidigare insamlad datatrafik. Den lagringstid som avses i bestämmelsen kan anses vara tillräcklig för att uppnå ovan avsedda mål.

Det bör fortfarande vidare betonas att verksamhet enligt paragrafen inte har som syfte att generera information om betydelseinnehållet i ett meddelande eller att följa hur den aktör som är föremål för åtgärden förflyttar sig, utan det handlar uttryckligen om att fastställa maximalt precisa sökbegrepp i anknytning till objektet. Om man förfar på ovan avsedda sätt, handlar det

om egentlig underrättelseinhämtning som avser datatrafik, för vilken ett i lagen avsett tillstånd ska inhämtas.

Till exempel ett protokollstack som använts som exempel i denna proposition kan jämföras med de uppgifter som inhämtats tidigare under tolv månader och på så sätt kan man få visshet om att ett protokollstack som fastställts som sökbegrepp riktas på rätt objekt. Lagringstiden kan anses vara nödvändig och skälig med beaktande av datatrafikens ständigt föränderliga karaktär och utvecklingen av tekniken och metoderna.

Det bör observeras att en militärunderrättelsemyndighet inte kan använda de här avsedda uppgifterna i något annat sammanhang, om inte en domstol beviljat tillstånd för en sådan befogenhet med vilken de här avsedda lagrade uppgifterna får behandlas. Således kan en militärunderrättelsemyndighet inte utreda till exempel identiteten på användaren av förmedlingsuppgifter eller meddelandets innehåll genom att använda 104 § i lagen om militär underrättelseverksamhet om inte uppgiften fått genom egentlig underrättelseinhämtning som avser datatrafik (68 eller 70 § i lagen). Således blir inte annan information än information som motsvarar sökbegreppen i domstolstillståndet inte föremål underrättelseinhämtning.

Lagring av datatrafik och tillträde till det förutsätter ett nytt datasystem och ett domstolstillstånd förutsätts för att få tillgång till de uppgifter som lagrats i det. Användningen av uppgifter ska registreras noggrant och övervakas noggrant såväl internt som externt.

Enligt momentet kan lagrade uppgifter användas i fastställandet av sökbegrepp enligt 1 mom. i paragrafen, men även för ett nedan reglerat syfte. Det sist nämnda hänvisar till egentlig underrättelseinhämtning som avser datatrafik enligt 68 och 70 § i lagen.

Enligt paragrafens 5 mom. kan lagrad tekniska data om datatrafik enligt 66 § 3 mom. användas för att fastställa sökbegrepp. I praktiken handlar det om jämförelse av uppgifter och att bilda ett användningsdugligt sökbegrepp och att jämföra ett identifierat sökbegrepp med tekniska historikdata.

67 b §. *Beslut om fastställande av sökbegrepp.* Enligt 1 mom. i paragrafen ska beslut om fastställande av sökbegrepp fattas av domstol på yrkande av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Bestämmelserna om beslutsfattande motsvarar vad som redan för närvarande föreskrivits om behandling av tekniska data. Den nya befogenheten handlar om behandling av datatrafik i dess mest tekniska form, varför även beslutsfattandet om den nya befogenheten motsvarar regleringen kring beslutsfattande om behandling av tekniska data.

Det föreslås att paragrafens 2 mom. innehåller bestämmelser om att giltighetstiden för ett tillstånd är högst sex månader från det datum då tillståndet getts eller det datum då beslutet fattats.

Enligt bestämmelsen kan tillståndet gälla även ovan konstaterade datum då tillståndet utfärdats eller tiden innan beslutet fattades, vilken kan vara längre än sex månader. I praktiken innebär detta en situation där man då sökbegrepp fastställs använder tekniska data enligt 66 § 2 mom. eller uppgifter enligt 67 a § 4 mom.

Paragrafens 3 mom. innehåller bestämmelser om de fakta som ska nämnas i ett yrkande och ett beslut. Enligt 1 punkten i momentet ska man i ett yrkande och ett beslut nämna det underrättelseuppdrag för vilket sökbegrepp fastställs och de fakta som gäller det. Enligt 10 § i lagen avses med 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 14 §. I beskrivningen av underrättelseuppdraget ska man specificera den större helhet om vilken sökbegrepp ska fastställas för att kunna använda underrättelseinhämtning som avser datatrafik på ett ändamålsenligt sätt.

Enligt 2 punkten i momentet ska man i ett yrkande och ett beslut nämna de fakta som ligger till grund för nödvändigheten att fastställa sökbegrepp. Som fakta kan man nämna till exempel att de sökbegrepp som används utifrån de gjorda observationerna inte längre producerar motsvarande information som tidigare fått med dem, men det utifrån erfarenheterna kan konstateras att kommunikationen sannolikt genomförs på ett annat sätt och att man inte får grepp om kommunikationen med de använda sökbegreppen.

Å andra sidan ska man i ett yrkande och ett beslut redogöra för varför sökbegreppen inte kan fastställas exempelvis genom att använda egentlig underrättelseinhämtning som avser datatrafik. I ett yrkande är det även möjligt att lägga fram en uppskattning av om man genom att fastställa sökbegrepp kan uppnå bättre och bättre riktad underrättelseinhämtning som avser datatrafik.

Enligt momentets 3 punkt ska man i ett yrkande och ett beslut nämna de förmodade regelbundenheter eller särdrag i objektets datatrafik på basis av vilka sökbegreppen fastställs och motiveringarna till dem.

Det datatrafikflöde som informationssystemen producerar har behandlats mer utförligt i den allmänna motiveringen i denna proposition. I datasystemen används flera olika system för att producera enskilda och gemensamma funktionaliteter i ett datasystem. I synnerhet i utspridda datasystem förutsätter datasystemets funktion kommunikation mellan anordningar som fysiskt finns på olika ställen, så att datasystemet som helhet fungerar på det önskade sättet.

För att elektronisk kommunikation ska dirigeras till det önskade målet på avsett sätt, behövs protokoll i datatrafiken. Protokollen bland annat delar upp en fil i en viss form och krypterar datatrafiken på ett visst sätt. Detta syns i datatrafikflödet i form av vissa regelbundenheter eller särdrag. Regelbundenheter och särdrag kan identifieras till exempel utifrån ett särdrag i verksamheten i ett enskilt protokoll som används i ett protokollstack, men ett egentligt sökbegrepp kan inte riktas utifrån detta.

Redan enbart de ovan beskrivna omständigheter som centralt påverkar datasystemets funktion genererar regelbundenheter och särdrag i informationssystemets datatrafik. Regelbundenheten eller särdraget enligt punkten kan vara kända från ett datasystem som redan utgör objekt, men det är känt att ett motsvarande datasystem används även av exempelvis en annan stats myndighet eller om information ska inhämtas från ett undersystem till huvudsystemet, vilket på grund av systemens interoperabilitet använder protokoll eller tekniker som åtminstone i hög grad motsvarar varandra än själva huvudsystemet. I detta skede är det dock inte ännu känt hur till exempel meddelandets avsändare och mottagare fastställs i datasystemet, varför ett noggrannare sökbegrepp inte ännu kan fastställas i detta skede.

Å andra sidan kan en regelbundenhet även ha sitt ursprung i den verkliga världen. Det kan till exempel vara känt att en militär övning ordnas i ett visst område och att meddelanden sänds under en viss tidpunkt under övningen. Om närmare sökbegrepp inte är kända, kan nya sökbegrepp fastställas utifrån datatrafiken i övningsområdet.

Ofta krävs manuellt arbete för att hitta datatrafik som motsvarar ett särdrag för att datatrafik som motsvarar en regelbundenhet eller ett särdrag ska hittas. Fastställande av sökbegrepp utifrån byteflödet i datatrafik förutsätter inte att datatrafiken packas upp i en form utifrån vilken en person utan avsevärt datatekniskt kunnande kan utreda innehållet i ett meddelande.

Enligt 4 punkten i momentet ska man i ett yrkande och ett beslut uppge de delar av ett kommunikationsnät som överskrider Finlands gräns, såsom de kabelfibrer mot vilka underrättelseinhämtning som avser datatrafik riktas för fastställandet av sökbegrepp.

Enligt 5 punkten i momentet ska man i ett yrkande och ett beslut nämna planen för fastställande av sökbegrepp. I planen ska man redogöra närmare för exempelvis hur fastställandet av sökbegrepp genomförs och med vilka metoder. I planen ska man även beskriva på vilket sätt maximalt lite betydelseinnehåll från kommunikationen når den mer ingående behandlingen och hur integritetsskyddet tillgodoses i så hög grad som möjligt.

Enligt 6 punkten i momentet ska man i ett yrkande och ett beslut nämna giltighetstiden för ett tillstånd med angivande av klockslag och enligt 7 punkten ska man nämna den med användningen av Försvarsmaktens underrättelsetjänsts metoder för underrättelseinhämtning särskilt förtrogn tjänsteman som leder och övervakar fastställandet av sökbegrepp.

Enligt momentets 8 punkt kan en domstol i sitt beslut fastställa begränsningar och villkor för underrättelseinhämtning som avser datatrafik. Om sådana begränsningar och villkor är kända redan då ett yrkande utarbetas, finns det skäl att skriva in dem redan i yrkandet. Begränsningar och villkor ska kunna ställas till exempel för hur Försvarsmaktens underrättelsetjänst får bilda sökbegrepp inom ramen för de kategorier av sökbegrepp för vilka domstolen beviljar tillstånd eller i vilken mån Försvarsmaktens underrättelsetjänst kan lagra datatrafik.

68 §. Underrättelseinhämtning som avser datatrafik hos statliga aktörer. Paragrafen och dess rubrik ändras så att paragrafen inte hänvisar till datatrafik hos statliga aktörer, utan till underrättelseinhämtning som avser datatrafik hos statliga aktörer. Praxis har visat att datatrafik hos en statlig aktör inte går genom vissa utvalda fibrer, utan bland den övriga datatrafiken. Den föreslagna formuleringen motsvarar bättre nuläget i fråga om datatrafiken rör sig.

Underrättelseinhämtning som avser datatrafik hos statliga aktörer kan fortfarande basera sig på användning av sökbegrepp.

Paragrafens 2 mom. ändras inte. Enligt bestämmelsen får Försvarsmaktens underrättelsetjänst behandla information som inhämtats om datatrafiken automatiskt och manuellt.

Paragrafens 3 mom. ändras. I och med ändring upphävs stryks det fullständiga förbudet att som sökbegrepp använda uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av en person som vistas i Finland eller som enligt förmodan används av honom eller henne. Det kan anses vara nödvändigt att göra denna strykning, eftersom en statlig aktör även kan befinna sig i Finland eller komma till Finland mitt under inhämtandet av information. I synnerhet i en situation där en statlig aktör befunnit sig utanför Finlands gräns och kanske till och med på ett överraskande sätt kommer till Finland, ska det vara möjligt att fortsätta underrättelseinhämtning som avser datatrafik hos statliga aktörer.

Bestämmelsen möjliggör inte att till exempel regleringen kring teleavlyssning kringgås. Med tanke på tillämpningen av bestämmelsen är det centralt att andra metoder för underrättelseinhämtning, såsom teleavlyssning, ska riktas mot objektet så fort som möjligt. Redan de allmänna principerna för militär underrättelseinhämtning, såsom

proportionalitetsprincipen, styr mot detta. Med exempelvis teleavlyssning får man dessutom i varje fall mer och närmare information om objektets kommunikation än genom underrättelseinhämtning som avser datatrafik. Man strävar efter att rikta andra metoder för underrättelseinhämtning mot objektet så fort som möjligt efter att objektets närmare vistelseplats har klarnat. Denna princip uttrycks i bestämmelsen genom en hänvisning till den temporära karaktären.

Till exempel i en situation där en specialgrupp från en främmande stats armé utgör föremål för underrättelseinhämtning som avser datatrafik hos en statlig aktör och gruppen anländer till Finland genom att dölja sina verkliga avsikter, är en förutsättning för att få närmare information om gruppen att bättre riktade metoder för underrättelseinhämtning används. Genom underrättelseinhämtning som avser datatrafik är det möjligt att i det initiala skedet få betydande information för att kunna använda bättre riktade metoder för underrättelseinhämtning i Finland.

Enligt paragrafens nya 4 mom. kan lagrad tekniska data om datatrafik enligt 66 § 3 mom. och lagrad datatrafik enligt 67 a § 3 mom. användas vid underrättelseinhämtning enligt paragrafen. I och med ändringen fås ännu noggrannare information om objektet och metoden för underrättelseinhämtning kan vidare riktas på ett ännu noggrannare sätt. Användningen av uppgifter förutsätter ett tillstånd enligt 69 §, i vilket man fastställt de sökbegrepp för uppgifter som man kan leta från de lagrade uppgifterna.

69 §. Beslut om underrättelseinhämtning som avser en statlig aktörs datatrafik. Paragrafens 2 mom. ändras. I enlighet med den gällande lagen är giltighetstiden för ett tillstånd sex månader, men tidsperioden börjar från det datum då tillståndet getts eller från och med det datum då beslutet fattats.

Enligt bestämmelsen kan tillståndet gälla även för uppgifter som lagrats utifrån föreslagna 66 § 3 mom. och 67 a § 3 mom.

70 §. Underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer. Paragrafens 2 mom. ändras. I fråga om underrättelseinhämtning som hänför sig till datatrafiken för någon annan än en statlig aktörs datatrafik undanröjs det absoluta förbudet att använda uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av en person som vistas i Finland eller som enligt förmodan används av honom eller henne (2 mom. i den gällande paragrafen). I och med att förbudet slopas kan även en person som deltar i ett allvarligt militärt hot eller ett allvarligt hot mot den nationella säkerheten och som vistas i Finland tillfälligt vara föremål för underrättelseinhämtning som avser datatrafik.

Föremålet för underrättelseinhämtningen är verksamhet som i väsentlig grad kan omfatta även personer som vistas i Finland. I synnerhet i en situation där en person med koppling till militär verksamhet eller verksamhet som allvarligt hotar den nationella säkerheten kommer till Finland på ett överraskande sätt under en tid då metoden för underrättelseinhämtning används, är det till en början möjligt att fortsätta underrättelseinhämtning som avser datatrafik, fram till dess att det är möjligt att övergå till bättre riktade metoder för underrättelseinhämtning, såsom teleavlyssning. Övergången till bättre riktade metoder för underrättelseinhämtning förutsätter redan att underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer är den sista metoden som får tillgripas i enlighet med 1 mom. i paragrafen, vilken även ska bedömas under användningen av underrättelseinhämtning som avser datatrafik. Till exempel i en situation där personal från armén eller underrättelsemyndigheter från en främmande stat har infiltrerat sig i Finland, är det å andra sidan möjligt att genom underrättelseinhämtning som avser datatrafik upptäcka detta, om personen är i kontakt med sin uppdragsgivaren över gränsen. Därefter kan en teleterminalutrustning eller teleadress som finns i Finland bevakas genom

underrättelseinhämtning som avser datatrafik fram till dess att bättre riktade metoder för underrättelseinhämtning kan användas.

Förbudet mot underrättelseinhämtning som avser datatrafik och som ska anses utgöra intern datatrafik i Finland förblir oförändrat.

Paragrafens 3 mom. ändras. Enligt momentet är det möjligt att i underrättelseinhämtning som avser någon annan än en statlig aktör använda även sökbegrepp som hänför sig till meddelandets innehåll.

Enligt definitionen av sökbegrepp (10 § 1 punkten) avses med sökbegrepp en uppgift som används för att vid underrättelseinhämtning som avser datatrafik så avgränsat och exakt som möjligt i en del av kommunikationsnätet selektera den datatrafik som är föremål för underrättelseinhämtningen, varvid intrånget i skyddet för hemligheten för förtroliga meddelanden sker endast i den omfattning som är nödvändig för att uppnå syftet med underrättelseinhämtningen. I nuläget kan det anses att användning av till exempel endast tekniska data om datatrafiken ofta producerar för breda sökresultat. De inhämtade uppgifterna kan redan i det initiala skedet avgränsas genom ett sökbegrepp i det semantiska innehållet.

Ett sökbegrepp som kan hänföra sig även till det semantiska innehållet i ett meddelande kan bedömas leda till att noggrannare information inhämtas från datatrafiken. Detta förbättrar integritetsskyddet i och med att underrättelseinhämtningen är noggrannare och bättre riktad och det överensstämmer bättre med definitionen av sökbegrepp i lagen. Det står dock klart att enbart användning av ett uttryck från det talade språket som sökbegrepp oftast producerar ännu mer omfattande resultat, vilket inte heller operativt sett kan anses vara förnuftigt. Språkliga sökbegrepp, såsom uttryck i det talade språket, används tillsammans med tekniska data som gäller datatrafiken i syfte att inhämta maximalt riktad information.

Slopandet av förbudet mot sökbegrepp som hänför sig till innehållet i ett meddelande har även en operativ betydelse. I nuläget är det möjligt att använda tekniska data om datatrafik som sökbegrepp. Tekniska data kan även finnas i innehållet i ett meddelande, till exempel i en e-posttråd som vidarebefordrats. I nuläget kan ett tekniskt sökbegrepp i sig anses rikta sig rätt genom att från datatrafikflödet avskilja datatrafik som motsvarar ett sökbegrepp, men denna avskiljning kan inte göras i fråga om huruvida sökbegreppet finns i meddelandets semantiska innehåll eller inte. På grund av detta måste underrättelsemyndigheten då den sätter sig in i datatrafik som motsvarar sökbegreppet med stöd av utplåningsskyldigheterna utplåna information där sökbegreppet förekommer, men information som motsvarar sökbegreppet finns i innehållet i ett meddelande, till exempel i ett vidarebefordrat e-postmeddelande. En uppgift som motsvarar ett sökbegrepp kan även finnas i uppgifter som i övrigt ska anses utgöra innehållet i ett meddelande i datatrafiken, såsom i en lista över kontaktuppgifter som lagras på en molnserver.

I och med den nu föreslagna ändringen kan information som når den fortsatta behandlingen gallras bort redan i det skede då sökbegrepp används, varvid till exempel den informationsmängd som inhämtas genom att använda vissa uttryck från det talade språket redan i utgångspunkten är mindre och bättre riktad. I nuläget blir den fortsatta behandlingen av datatrafiken enligt sökbegreppen således en del av den fas där datatrafik filtreras bort från datatrafiken med hjälp av sökbegrepp. Således når mindre information militärunderrättelsemyndighetens fortsatta behandling.

Användning av uppgifter i det semantiska innehållet som sökbegrepp ska motiveras i den ansökan som ska göras till domstolen i enlighet med 71 § 3 mom. 5 punkten. I motiveringen

kan man föra fram till exempel hurudana observationer som tidigare gjorts om objektets datatrafik, till exempel om objektet använder vissa ord eller uttryck eller ett särskilt språk i sin kommunikation i sin verksamhet.

Paragrafens 4 mom. förblir samma som i nuläget.

Paragrafens 5 mom. är nytt. Enligt det är det möjligt att i underrättelseinhämtning som hänför sig till en annan än en statlig aktör använda tekniska data enligt 66 § 3 mom. och datatrafik som använts för att fastställa sökbegrepp med stöd av 67 a § 3 mom. Ett tillstånd enligt 71 § förutsätts för att använda uppgifterna. Användningen av lagrade uppgifter baserar sig på användningen av de sökbegrepp som konstaterats i tillståndet.

71 §. *Beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer.* Paragrafens 2 mom. ändras. I enlighet med den gällande lagen är giltighetstiden för ett tillstånd sex månader, men tidsperioden börjar från det datum då tillståndet getts eller från och med det datum då beslutet fattats.

Enligt bestämmelsen kan tillståndet gälla även tiden innan ovan konstaterade datum då tillståndet utfärdats eller beslutet fattades, vilken kan vara längre än sex månader. I praktiken innebär detta en situation där man använder uppgifter som lagrats utifrån föreslagna 66 § 3 mom. och 67 a § 3 mom. i underrättelseinhämtning som avser datatrafik.

74 §. *Utlämnande av uppgifter om ett skadligt datorprogram till företag och sammanslutningar.* Det föreslås att paragrafen upphävs eftersom den är obehövlig. Uppgifter om ett skadligt datorprogram kan lämnas ut utifrån den föreslagna ändringen av 18 § 2 mom.

77 §. *Tryggande av en tjänsteman som använder en metod för underrättelseinhämtning.* Paragrafens 1 mom. innehåller bestämmelser om tryggande av en tjänsteman som använder en metod för underrättelseinhämtning. Tryggandet kan ske genom att förse en tjänsteman som använder de metoder för underrättelseinhämtning som nämns i bestämmelsen med anordningar som möjliggör avlyssning eller observation. Bestämmelsen gäller alltså för anordningar som en tjänsteman bär.

Utöver det ovan konstaterade kan tryggandet av en tjänsteman ske även genom att installera en anordning som möjliggör avlyssning och observation i ett utrymme som används av tjänstemannen. Detta minskar för egen del risken för att tjänstemannen avslöjas, eftersom anordningar i kläder i vissa situationer kan avslöjas jämförelsevis enkelt. Dessutom ger anordningarna i utrymmet möjlighet att få en bredare lägesbild av själva situationen, eftersom utrymmet kan övervakas på ett mer övergripande sätt. Således är det exempelvis möjligt att få visshet om att en tjänsteman som använder en metod för underrättelseinhämtning inte utsätts för angrepp bakifrån.

I paragrafens 2 mom. görs inga ändringar. Det är tillåtet att spela in avlyssning och observation, men upptagningarna ska utplånas direkt efter att de inte längre behövs för att trygga en tjänsteman. Om det dock finns ett behov av att förvara dessa på grund av orsaker relaterade till rättsskyddet i ärendet, får upptagningarna förvaras och användas i detta syfte. I så fall ska upptagningarna utplånas då ärendet har avgjorts på ett lagakraftvunnet sätt eller avvisats.

Det står klart att paragrafen inte möjliggör att bestämmelserna om metoder för underrättelseinhämtning kringgås.

78 a §. *Tryggande av informationskällans liv och hälsa.* Paragrafen är ny. Till den flyttas 78 § 5 mom. i den gällande lagen, enligt vilket huvudstabens underrättelsechef får besluta att en informationskälla ges, för användning i ett enskilt fall, bland annat falska handlingar, om det är nödvändigt för att skydda informationskällans liv och hälsa. Avsikten är inte att ändra detta rättsläge.

Bestämmelsen gäller situationer där de nämnda uppgifterna och handlingarna används för att skydda informationskällans liv och hälsa i en annan situation än för att föra informationskällan till Finland.

Regleringen i paragrafens 2 mom. är ny. Till lagen fogas en bestämmelse som innebär att en militärunderrättelsemyndighet även har en möjlighet att arrangera så att en informationskälla kan korsa Finlands gräns på annat sätt. Det handlar dock inte i samtliga fall om inresa i landet via ett normalt gränsövergångsställe, utan om att en informationskälla kommer till Finland i smyg vid behov. Bestämmelsen täcker även situationer där informationskällan ordnas till Finland genom att använda i 1 mom. avsedda falska uppgifter eller handlingar.

Det finns bestämmelser om ordnande av olaglig inresa i 17 kap. 8 § i strafflagen. Till exempel enligt 1 mom. 2 punkten ska man för ordnande av olaglig inresa döma den som för in eller försöker föra in en sådan utlänning i Finland, eller genom Finland till ett annat land, som har ett dokument för inresa som är falskt eller förfalskat eller har beviljats någon annan, eller som har fått av en myndighet genom att ge osanna eller vilseledande uppgifter som är betydelsefulla för beviljandet av dokumentet, genom att muta myndigheten eller genom våldsam motstånd mot tjänsteman. Hänvisningen till paragrafen i strafflagen förtydligar även regleringen i bestämmelsen i fråga om den redan för närvarande reglerade användningen av falska handlingar och uppgifter. Den föreslagna hänvisningen undanröjer på ett tydligt sätt det straffrättsliga ansvaret i de situationer som bestämmelsen avser.

Med ordnande enligt det förslag till bestämmelse som nu behandlas avses vad som avses i 17 kap. 8 § i strafflagen. Således får militärunderrättelsemyndigheten till exempel 1) för in en sådan utlänning i Finland, eller genom Finland till ett annat land, som inte har ett resedokument, visum, uppehållstillstånd eller något annat med ett resedokument jämförbart dokument som krävs för inresa, 2) föra in en sådan utlänning i Finland, eller genom Finland till ett annat land, som har ett dokument som är falskt eller förfalskat eller har beviljats någon annan eller 3) ordna eller förmedla transport till Finland för en ovan avsedd utlänning.

I princip ska militärunderrättelsemyndigheten i mån av möjlighet sträva efter att skydda informationskällan. I normala fall handlar det om att man inte begär att informationskällan inhämtar information på ett sätt som tydligt orsakar en fara för hans eller hennes liv och hälsa. Situationerna kan dock förändras snabbt och beroende på hurdan information informationskällan har tillgång till, kan hot för att källans liv och hälsa äventyras vara verkligt.

I den nu behandlade situationen har till exempel en person med en hög position i samhället i målstaten delat betydande sekretessbelagda uppgifter till militärunderrättelsemyndigheten. I något skede av det relativt långa samarbetet börjar informationskällan starkt misstänka att målstatens myndigheter börjat följa hans eller hennes förehavanden. En närmare uppföljning av situationen styrker observationen. Det är allmänt känt att målstatens myndigheter torterar fångar och även i detta fall kan det förmodas att informationskällan kommer att torteras, till och med till döds. Utifrån de mottagna uppgifterna förbereds falska handlingar för informationskällan och falska registeranteckningar görs i de behövliga myndighetsregistren. Med hjälp av de utarbetade handlingarna och registeranteckningarna kan informationskällan korsa Finlands

gräns via ett gränsövervakningsställe och vidare till en tredje stat med hjälp av den behöriga myndigheten i denna stat.

Å andra sidan kan situationen i målstaten vara sådan att staten strikt övervakar avlägsnandet ur landet. Det kan krävas separata handlingar av myndigheterna i målstaten för att avlägsna sig ur landet. I en situation där informationskällan är exempelvis en välkänd person i målstaten eller åtminstone välkänd bland myndigheterna, räcker förfälskade handlingar inte nödvändigtvis för att skydda informationskällans liv och hälsa. Således är det möjligt att skyddet av informationskällans liv och hälsa kan förutsätta att passeringen av Finlands gräns sker annanstans än via ett officiellt gränsövergångsställe.

I en situation där man fått starka bekräftade uppgifter om att informationskällan avslöjats av målstaten, kan militärunderrättelsemyndigheten förbereda en plan för att informationskällan ska kunna korsa Finlands gräns. I planen är det möjligt att markera ut en rutt i terrängen på en karta, via vilken informationskällan kan korsa Finlands landsgräns. Planen kan även innehålla uppgifter om när landsgränsen kan korsas på så sätt att de andra myndigheterna inte upptäcker det.

Enligt 17 kap. 8 § 2 mom. i strafflagen betraktas som ordnande av olaglig inresa inte en gärning som bedömd som en helhet bör anses ha begåtts av godtagbara skäl, särskilt med beaktande av gärningsmannens bevekelsegrunder när dessa har samband med humanitära skäl eller nära familjeförhållanden samt sådana förhållanden i utlänningens hemland eller i det land där han eller hon stadigvarande är bosatt som påverkar hans eller hennes säkerhet. I de nu behandlade situationerna blir ovan avsedda bestämmelse i strafflagen med säkerhet tillämplig, men på grund av regleringens tydlighet kan det anses vara ändamålsenligt att uttryckligen utesluta brott.

Det kan bedömas att tillämpningen kommer att vara exceptionell. Möjligheten att ordna inresa i landet på ett avvikande sätt kan anses förbättra förtroendet för den finländska militära underrättelseverksamheten och det finländska samhället hos en informationskälla. I praktiken ska även en informationskälla vara väldigt pålitlig och de uppgifter som han eller hon har överlämnat ska vara betydelsefulla för att det ska bli aktuellt att tillämpa bestämmelsen.

Nödvändighet är en förutsättning för att bestämmelsen ska tillämpas. Nödvändighet förutsätter att det inte är möjligt att trygga en informationskälla med andra metoder eller att det kräver avsevärda resurser. Dessutom ska det vara möjligt att bedöma att behovet av att skydda en informationskällas liv och hälsa är verkligt.

Bedömningen ska vara omfattande och basera sig på säkerställda uppgifter. En övergripande bedömning av mållandet kan göras till exempel utifrån de allmänt tillgängliga uppgifterna, såsom att det är allmänt känt att målstatens myndigheter gör sig skyldiga till tortyr eller annan omänsklig behandling av fångar. Den närmare bedömningen ska basera sig på bekräftade uppgifter exempelvis om att man upptäckt att informationskällan observeras av de lokala myndigheterna. Ofta är det inte nödvändigtvis tillräckligt att man upptäcker spaning, utan målstatens myndigheter ska även vidta andra mer konkreta åtgärder, såsom husrannsakingar eller samtal med källan, innan nödvändighetskriteriet utifrån en helhetsbedömning kan anses vara uppfyllt.

De situationer som avses i förslaget är synnerligen sensitiva, vilket å sin sida innebär att information inte kan delas till de andra myndigheterna. Å andra sidan kan fallen i förslagen även vara utrikes- och säkerhetspolitiskt känsliga, varvid den utrikes- och säkerhetspolitiska ledningen ska ha den behövliga informationen.

En informationskälla kan söka asyl i Finland, varvid han eller hon går igenom den normala processen för asylsökanden. Finland kan även användas som transiteringsland till ett tredje land.

Det föreslås att paragrafens 3 mom. innehåller bestämmelser om rätten för en informationskälla att använda uppgifter, registeranteckningar och handlingar enligt 1 mom. i de situationer som avses i paragrafens 2 mom. Paragrafens 2 mom. innehåller bestämmelser om militärunderrättelsemyndighetens rätt att ordna in en informationskälla i landet, men detta undanröjer inte ett eventuellt straffrättsligt ansvar för informationskällan.

Bestämmelsen gäller i synnerhet för situationer där informationskällan kommer till landet genom att använda falska registeranteckningar, uppgifter och handlingar vilka getts och framställts av militärunderrättelsemyndigheten eller genom att använda ett annat än ett officiellt övergångsställe med hjälp av militärunderrättelsemyndigheten. I den första situationen handlar det om en situation enligt 17 kap. 7 § 1 punkten i strafflagen där informationskällan passerar eller försöker passera Finlands gräns utan något resedokument, visum, uppehållstillstånd eller annat dokument som jämföras med ett resedokument vilket berättigar detta. I och med det nu behandlade förslaget till bestämmelse kan en informationskälla i samband med en gränspassering använda falska uppgifter, registeranteckningar och handlingar vilka utarbetats och framställts av militärunderrättelsemyndigheten utan att begå ett brott.

I det sist nämnda fallet handlar det om situationer enligt 17 kap. 7 § 1 punkten i strafflagen där informationskällan passerar eller försöker passera Finlands gräns från ett annat ställe än ett lovligt inrese- eller utreseställe. Paragrafens 2 mom. innehåller bestämmelser om rätten för militärunderrättelsemyndigheten att ordna en informationskälla till Finland utan hinder av 17 kap. 8 § i strafflagen. I situationer enligt paragrafens 2 mom. gör sig informationskällan inte skyldig till ett riksgränsbrott då han eller hon passerar Finlands gräns via ett annat än ett lovligt inreseställe.

De åtgärder som avses i bestämmelsen kan även avse andra än de gärningsformer som avses i 7 § 1 mom. Riksgränsbrott kan begås av den som i enlighet med 2 punkten annars bryter mot bestämmelserna om överskridande av gränsen eller på det sätt som avses i 3 punkten i strid med 51 § i gränsbevakningslagen eller utan tillstånd som avses i 52 § i den lagen vistas eller färdas inom gränszonen eller vidtar någon åtgärd som är förbjuden inom den. En informationskälla enligt bestämmelsen kan bli tvungen att vänta till exempel på att upphämtas av militärunderrättelsemyndigheten vid gränszonen till exempel utan något tillstånd enligt 52 § i gränsbevakningslagen.

Det är även möjligt att en informationskällas ankomst till Finland enligt paragrafen uppfyller rekvisitet för ett annat brott. I synnerhet genom att använda en falsk handling kan en informationskälla göra sig skyldig exempelvis till registeranteckningsbrott enligt 16 kap. 7 § i strafflagen eller lämnande av oriktiga personuppgifter enligt 16 kap. 5 § i strafflagen. Ovan avsedda bestämmelser kan anses innehålla reglering, med stöd av vilken informationskällan i de nu behandlade situationerna inte gör sig skyldig till brott.

82 §. Förbud mot underrättelseinhämtning. Till paragrafens 1 mom. fogas teknisk observation av utrustning och underrättelseinhämtning i Finland som avser en statlig aktörs datasystem som metoder för underrättelseinhämtning. I och med de föreslagna ändringarna utvidgas förbudet i 1 mom. att rikta de metoder för underrättelseinhämtning som nämns i momentet till särskilda yrkesgrupper. Teknisk observation av utrustning kan även hänföras till lagrad kommunikation och den nya befogenheten, underrättelseinhämtning i Finland som avser en statlig aktörs datasystem, kan på motsvarande sätt hänföras till kommunikation.

På grund av motsvarande orsaker fogas på motsvarande sätt ovan nämnda metoder för underrättelseinhämtning till 2 mom. i paragrafen.

85 §. Avbrytande av användningen av en metod för underrättelseinhämtning. Paragrafen ändras. Redan den gällande paragrafen innehåller omfattande bestämmelser om avbrytande av användningen av vissa metoder för underrättelseinhämtning, men det finns ett behov av att utveckla bestämmelsen. Paragrafen handlar främst om en förtydligande bestämmelse. Redan för närvarande har lagen om militär underrättelseverksamhet tolkats på så sätt att teleavlyssning och teleövervakning ska avbrytas så fort som möjligt till den del som underrättelseinhämtningen hänför sig till ett annat meddelande från objektet eller ett annat meddelande som är avsett för honom eller henne. Upptagningar som fåtts genom avlyssning och uppgifter som fåtts genom teleövervakning samt anteckningar om de mottagna uppgifterna ska utplånas utan dröjsmål.

I 1 mom. i paragrafen föreskrivs att om teleavlyssningen eller teleövervakningen riktas mot något annat än i tillståndet avsett meddelande från eller till den person som är föremål för tillståndet eller att den person som är föremål för den tekniska avlyssningen riktas mot inte befinner sig i det utrymme eller på den plats som avlyssnas, ska användningen av metoden för underrättelseinhämtning avbrytas så snart som möjligt, och de upptagningar som har fåtts genom avlyssningen och anteckningarna om de uppgifter som fåtts genom den ska genast utplånas. Bestämmelsen motsvarar det gällande momentet, med den skillnaden att teleövervakning fogas till den.

Paragrafens 2 mom. gäller radiosignalspaning. Bestämmelsen motsvarar 2 mom. i den gällande paragrafen. Enligt paragrafen om radiosignalspaning är det genom radiosignalspaning inte tillåtet att inhämta information från innehållet i ett meddelande från en annan än en statlig aktör. På grund radiosignalspaningens natur är det möjligt att kommunikation som åtnjuter skyddet för ett förtroligt meddelande blir objekt för den. Enligt det nu behandlade momentet ska ett sådant meddelande och anknutna anteckningar utplånas direkt. I detta fall avser inte avbrytande att all radiosignalspaning avbryts, utan radiosignalspaningen ska till denna del riktas på nytt, på så sätt att den statlig aktörens upptäckta kommunikation inte längre når radiosignalspaningen.

Enligt paragrafens 3 mom. gäller skyldigheten att avbryta åtgärder och att utplåna upptagningarna och anteckningarna också teknisk observation av utrustning. Teknisk observation av utrustning kan hänföra sig till ett meddelande som förvaras. Om det kommer fram att den tekniska observationen av utrustning hänför sig till ett förtroligt meddelande, på vilket teleavlyssning enligt 4 kap. i lagen ska tillämpas, teleövervakning eller annan teknisk observation än teknisk observation av utrustning ska tillämpas, ska den tekniska observationen av utrustning avbrytas och de uppgifter som fåtts till denna del och anteckningarna om uppgifterna utplånas direkt.

Bestämmelsen kan anses vara central på grund av den föreslagna ändringen som gäller teknisk observation av utrustning, i och med att teknisk observation av utrustning kan riktas även på personbasis. I sig finns det redan en gällande bestämmelse om riktande av en metod på personbasis, i vilken det konstateras att om det kommer fram att en person enligt 32 § 4 mom. i lagen inte längre använder en anordning eller programvara som är föremål för teknisk observation av utrustning, ska den tekniska observationen av utrustning avbrytas.

På ett sätt som motsvarar paragrafens 4 mom. ska underrättelseinhämtning i Finland som avser statliga aktörers datasystem avbrytas till den del som den observeras hänföra sig till en anordning, en anordning för informationsöverföring eller en programvara som behandlar data, vilken inte är en del av objektets datasystem. De mottagna uppgifterna och upptagningarna samt anteckningarna om dessa ska utplånas direkt.

Det föreslås att paragrafens 5 mom. på ett sätt som motsvarar 4 och 5 mom. i den gällande paragrafen om avbrytande av platsspecifik underrättelseinhämtning. Till det föreslagna momentet sammanslås 4 och 5 mom. i den gällande paragrafen, vilka gäller avbrytande av platsspecifik underrättelseinhämtning.

86 §. Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik. Till paragrafens 1 mom. fogas en ny punkt, enligt vilken information ska utplånas, om det kommit fram att informationen inte behövs för landets försvar eller för att skydda den nationella säkerheten. Skyldigheten till utplåning enligt bestämmelsen gäller således för information som är oväsentlig för landets försvar eller för att skydda den nationella säkerheten.

I vissa fall kan information som fås genom underrättelseinhämtning som avser datatrafik gälla ett annat hot mot landets försvar eller annan verksamhet som allvarligt hotar den nationella säkerheten av objektet för underrättelseinhämtning som avser datatrafik än det hot eller den verksamhet som lett till att ett tillstånd till underrättelseinhämtning som avser datatrafik har beviljats. Det kan till exempel handla om att ett tillstånd till underrättelseinhämtning som avser datatrafik har beviljats för att inhämta information om ett militärt hot, men man genom den underrättelseinhämtning som avser datatrafik som genomförts med stöd av tillståndet i stället för information om det egentliga objektets trafik får information om sådan verksamhet som allvarligt hotar Finlands vitala funktioner. Om sådan information som fås som en biprodukt av tillståndspliktig underrättelseinhämtning som avser datatrafik är av betydelse för landets försvar eller för skyddet av den nationella säkerheten, föreligger ingen skyldighet att utplåna den.

Bestämmelsen motsvarar vad som föreskrivits om skyddspolisens skyldighet att utplåna information i 15 § i lagen om civil underrättelseinhämtning avseende datatrafik.

Trots ovan avsedda tillägg, som ska anses vara av teknisk natur och som förtydligar bestämmelsen, förblir paragrafen i samma form som i nuläget i fråga om tillämpningen av den; en militärunderrättelsemyndighet får fortsättningsvis inte lagra uppgifter som är onödiga för dess uppgifter. Inhämtad information ska granskas aktivt och utplånas utan dröjsmål.

Vad som föreskrivs i paragrafen gäller inte för uppgifter som lagrats utifrån 66 § 2 mom. och 67 a § 4 mom.

89 §. Skyldighet att underrätta. Den gällande paragrafen kan författningstekniskt sett inte anses vara ändamålsenlig. Därför sprids bestämmelserna i paragrafen till nya 89 a § och 89 b §. Paragrafens 1 mom. förblir oförändrad och 7 mom. i den gällande paragrafen övergår till att vara 2 mom. i paragrafen.

Det föreslås att en ny bestämmelse fogas till paragrafen. Nya 3 mom. innehåller bestämmelser om en underrättelse i situationer på vilka 10 kap. 60 § 3 mom. i tvångsmedelslagen tillämpas. I dessa situationer är det möjligt att en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman yrkar på att man skjuter upp eller avstår från underrättelsen. Detta behov beror på att den gällande lagen om militär underrättelseverksamhet, i motsats till exempelvis 5 kap. 58 § 5 mom. i polislagen och 5 a kap. i polislagen, inte innehåller något omnämnande om att tvångsmedelslagen kan tillämpas i tillämpliga delar. På grund av detta blir den paragraf till vilken det hänvisas tillämplig i oförändrad form i enlighet med dess ordalydelse i fråga om lagen om militär underrättelseverksamhet, varvid en anställningsberättigad tjänsteman ska yrka på uppskov eller att underrättelsen inte ges.

Hänvisningen till påbörjad förundersökning i bestämmelsen innebär uttryckligen i fråga om en person som är föremål för förundersökning att han eller hon ansluter sig till verksamheten vid ett underrättelseobjekt.

Den gällande paragrafens 8 mom., som gäller underrättelse till en statlig aktör, övergår till att bli paragrafens 4 mom.

89 a §. *Underrättelse om användning av underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer.* Paragrafen är ny. Det föreslås att paragrafen innehåller bestämmelser om att man i princip inte gör någon underrättelse om underrättelseinhämtning som avser datatrafik hos statliga aktörer. I fråga om en statlig aktör utfärdas bestämmelser om mer omfattande avstående från underrättelsen i föreslagna 89 § 4 mom., som motsvarar 89 § 8 mom. i den gällande lagen.

I egenskap av definition avviker underrättelseinhämtning som avser datatrafik från till exempel teleavlyssning och det är inte en lika effektiv metod för underrättelseinhämtning som teleavlyssning för objektet. Underrättelseinhämtning som avser datatrafik avgränsas fysiskt genom att rikta den till en viss del av ett kommunikationsnät som överskrider Finlands gräns. Så som redan konstaterats, går datatrafiken i respektive situation längs med den effektivaste rutten i kommunikationsnätets delar och därför kan det konstateras att slumpmässig datatrafik blir föremål i ett system för underrättelseinhämtning som avser datatrafik. Information som är signifikativ för underrättelseverksamhet fås dock även från annat innehåll än innehållet i det egentliga meddelandet.

Underrättelseinhämtning som avser datatrafik är i princip avsedd för underrättelseinhämtning som gäller hot med ursprung bakom den finska gränsen. Även på grund av denna utgångspunkt är det i praktiken omöjligt att på personnivå utreda den ursprungliga avsändaren av datatrafik som kommer från utlandet eller hans eller hennes hemvist, varvid det i praktiken är omöjligt att göra en underrättelse. Dessutom är det inte möjligt att förmoda att en militärunderrättelsemyndighet för något täckande register över de aktörer som ska ges en underrättelse i en situation där de kommer till Finland.

Hur underrättelseinhämtning som avser datatrafik riktas till slut baserar sig på sökbegreppen och kategorierna av sökbegrepp. I synnerhet kategorierna av sökbegrepp utgörs av omfattande sökbegrepp som hänför sig till objektet. Underrättelseinhämtning som avser datatrafik hänför sig inte till en viss person, utan till hotet. På grund av detta är det inte möjligt att prata på samma sätt om verksamhet som ingriper i skyddet för privatlivet och privata meddelanden eller om underrättelseinhämtning av motsvarande intensitet som vid exempelvis sedvanlig teleavlyssning.

Så som konstaterats tidigare har Europadomstolen godkänt underrättelsesystem som saknar en principiell underrättelseskyldighet. Europadomstolen har i sina avgöranden konstaterat att i synnerhet i fråga om underrättelseinhämtning som avser datatrafik är det i praktiken omöjligt att göra en underrättelse och att man kan anse att det är ett tillräckligt skydd att en person kan överföra sitt ärende för utredning genom andra metoder. Detta kan även vara ett effektivare alternativ för personen.

Syftet med underrättelseskyldigheten är att målpersonen kan förlita sig på behövliga rättsskyddsmedel och överföra lagenligheten i en myndighets verksamhet för prövning. I princip reducerar dock inte den föreslagna ändringen av underrättelseskyldigheten i fråga om hemlig underrättelseinhämtning de facto rätten för personerna att få sin sak undersökt, eftersom var och en utifrån 12 § i lagen om övervakning av underrättelseverksamheten, åtminstone om man så

misstänker, har rätt att framföra en begäran om att underrättelsetillsynsmyndigheten undersöker om en eventuell metod för underrättelseinhämtning som riktats mot honom eller henne varit lagenlig. I 11 § i den nämnda lagen föreskrivs därtill att klagomål till underrättelsetillsynsombudsmannen kan i ett ärende som omfattas av ombudsmannens övervakningsbehörighet anföras av var och en som anser att hans eller hennes rättigheter har kränkts vid underrättelseverksamhet eller att det annars har förfarits lagstridigt i underrättelseverksamheten. I fråga om underrättelseskyldigheten bör det konstateras att Europadomstolen även i princip godkänt avstående från underrättelse, om personen har tillgång till motsvarande metoder, såsom en extern övervakande aktör, via vilken personen kan nå ett motsvarande slutresultat som via underrättelseskyldigheten.

Till övriga delar utplånas i enlighet med den gällande bestämmelsen ett meddelande som inkommit till ett system för underrättelseinhämtning som avser datatrafik i enlighet med utplåningsskyldigheterna och således uppkommer inte någon principiell underrättelseskyldighet. Detta föreskrivs uttryckligt i 4 mom.

Eftersom objektet för militär underrättelseinhämtning kan vara en privat sammanslutning i anknytning till en främmande stats väpnade styrkor, är personen således i sig inte av betydelse, utan objektet för underrättelseinhämtning som avser datatrafik är en organisation; på grund av naturen på underrättelseinhämtning som avser datatrafik är det överhuvudtaget inte ofta möjligt att anse att målpersoner som kan urskiljas tydligt utgör föremålet.

Enligt paragrafens 2 mom. ska en underrättelse göras om man vid underrättelseinhämtning som avser datatrafik utrett eller det i sådan kommit fram information som omfattas av vittnesförbud eller rätt att vägra vittna för de aktörer som avses i 82 § 1 mom. Bestämmelsen gäller bland annat präster och journalister.

Kommunikationen mellan de aktörer som nämnts i bestämmelsen och de uppgifter som de behandlar kan anses vara synnerligen förtroliga. Om en sådan instans som nämns i bestämmelsen deltar i verksamhet som är föremål för användning av en metod för underrättelseinhämtning, föreligger dock inte någon underrättelseskyldighet.

Underrättelseskyldighet föreligger dock inte om uppgiften utplånats utifrån 81 eller 86 § i enlighet med hänvisningen i momentet. Om en uppgift utplånats på grund av att den inte behövs, kan en underrättelseskyldighet naturligtvis inte heller uppstå. Paragrafen motsvarar 86 § 2 mom. i den gällande lagen.

89 b §. *Lämnande av underrättelse, uppskjutande av underrättelse samt avstående från underrättelse.* Paragrafen är ny. Utöver de materiella ändringarna överförs vissa bestämmelser från gällande 89 § för att tydliggöra lagens systematik.

Enligt paragrafens 1 mom. ska en underrättelse till en person som avses i 89 § eller 89 a § göras utan dröjsmål skriftligen efter det att syftet med användningen av en ovan avsedd metod för underrättelseinhämtning har nåtts. Underrättelsen ska dock göras till en person enligt de paragrafer till vilka det hänvisats ovan senast ett år efter att användningen av metoden för underrättelseinhämtning avslutats. Bestämmelsen motsvarar gällande 89 § 1 mom.

Enligt paragrafens 2 mom. blir underrättelseskyldigheten konkret först då identiteten på den som varit föremål för en metod för underrättelseinhämtning har klarnat. Naturligtvis är det i praktiken omöjligt att göra en underrättelse utan information om identiteten.

Dessutom ska man känna till personens bostadsort i Finland. Enkom att identiteten är känd räcker inte för att göra en skriftlig underrättelse, utan man ska känna till personens bostadsort eller en annan adress dit underrättelsen kan skickas. Först efter att de två ovan nämnda uppgifterna har klarnat är det möjligt att göra en underrättelse.

Om man inte känner till bostadsorten för ett objekt för användning av metoder för underrättelseinhämtning vars identitet är känd, förutsätts inte särskilt omfattande åtgärder av militärunderrättelsemyndigheten enkom för att göra underrättelsen. På motsvarande sätt förutsätts inte omfattande utredningsåtgärder för att utreda ett objekt vars identitet inte är känd. Omfattande utredningar för att göra underrättelsen kan i onödan äventyra skyddet för personens integritet.

Även i fråga om paragrafens 2 mom. bör det observeras att var och en som misstänker sig ha blivit föremål för en metod för underrättelseinhämtning kan överföra sitt ärende för att utredas av underrättelsetillsynsombudsmannen.

Enligt 3 mom. i paragrafen 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. Bestämmelsen motsvarar gällande 89 § 5 mom.

Enligt paragrafens 4 mom. får domstolen på yrkande av huvudstabens underrättelsechef eller en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman besluta att en underrättelse till objektet 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 skyddet av Finlands militär landsförsvar eller för att garantera den nationella säkerheten eller skydda liv eller hälsa. Domstolen får besluta att underrättelsen helt ska utebli, om det är nödvändigt för att trygga det militära försvaret av landet eller för att säkerställa 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 till exempel 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. Inhämtandet av information ska kunna anknyta till vilken som helst pågående underrättelseoperation, också till en civil underrättelseoperation.

Uppskov ska också vara möjligt med tanke på landets försvar eller skyddandet av den nationella säkerheten. Detta innebär att det måste föreligga 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. Paragrafen motsvarar 89 § 6 mom. i den gällande lagen.

I 5 mom. i paragrafens finns det bestämmelser om när en underrättelse inte görs. Bestämmelsen avskiljs till ett eget moment från gällande 89 § 6 mom. Bestämmelsen motsvarar den gällande bestämmelsen till denna del.

Enligt momentet får underrättelsen utifrån en domstols beslut 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.

I 6 mom. föreslås en hänvisning till domstolsförfarandet. Ifall domstolen inte beviljar uppskov eller godkänner att en underrättelse helt uteblir, ska den som framställt yrkandet kunna framföra klagomål om beslutet hos Helsingfors hovrätt på det sätt som föreskrivs i 113 §.

91 §. *Befogenheter för den som inte arbetar i tjänsteförhållande.* Den gällande regleringen gäller endast reservister som genomgått tillräcklig utbildning och som deltar i repetitionsövningar enligt värnpliktslagen. Dessutom har användningen av metoder för underrättelseinhämtning avgränsats till radiosignalspaning, underrättelseinhämtning som avser utländska datasystem, behandling av tekniska data och riktande av underrättelseinhämtning som avser datasystem. Paragrafen ändras på så sätt att det vid militär underrättelseinhämtning i en ännu större omfattning är möjligt att använda personer i en tjänst enligt värnpliktslagen och personer som deltar i det frivilliga landsförvaret. Dessutom har ovan avsedda personer en möjlighet att använda metoder för underrättelseinhämtning i en ännu större omfattning. Det står dock klart att personer i en tjänst enligt värnpliktslagen och personer som deltar i en frivillig övning inte kan användas för att åtgärda personalbrist, utan det ska finnas en försvarsmaktsrelaterad orsak till tjänsten eller den frivilliga övningen. De särskilda skälen kan vara till exempel kunskaper i sällsynta språk i Finland och annat specialkunnande om en viss ärendehelhet.

I de situationer som avses i bestämmelsen handlar det om ett så kallat grått skede, varvid lindrigare åtgärder inom omfattande påverkan riktar sig mot landets försvar och den nationella säkerheten och en eventuell militär operation förbereds. Ur den militära underrättelseinhämtningens synvinkel innebär detta att organisationen ska utökas snabbt och att flera arbetstagare behövs, dock för en kort tid om händelserna utvecklas i en bra riktning.

I paragrafens 1 mom. hänvisar man för det första till en tjänst enligt värnpliktslagen. Med detta avses utöver beväringstjänsten, repetitionsövningar, extra tjänstgöring och mobilisering. Den som förordnats till tjänstgöring kan användas i uppdrag inom militär underrättelseinhämtning med de begränsningar som föreskrivs nedan.

Till momentet fogas även en möjlighet att använda personer som deltar i en frivillig övning enligt 18 och 19 § i lagen om frivilligt försvar. Den nämnda lagens 18 § gäller frivilliga övningar som ordnas av Försvarsmakten.

Lagens 19 § gäller specialuppdrag under frivilliga övningar som ordnas av Försvarsmakten. Även andra personer än de som avses i 18 § kan delta i övningar enligt paragrafen, så länge som de i fråga om hälsa och andra personliga egenskaper lämpar sig för dessa. Enligt bestämmelsen är en förutsättning inte att beväringstjänsten avlagts eller hörande till reserven. Via frivilliga övningar är det möjligt att i militär underrättelseinhämtning i en ännu mer omfattande grad inkludera kunnande från samhällets olika delområden.

Tillräcklig utbildning för de fastställda uppgifterna förutsätts av personer i en tjänst enligt värnpliktslagen och personer som deltar i det frivilliga landsförvaret. Militärunderrättelsemyndigheten fastställer vad som är tillräcklig utbildning och erfarenhet för

den aktuella uppgiften. Vid förfarande i underrättelsehelheten är erfarenhet naturligtvis en förutsättning för övergång till mer krävande uppgifter och de tillgängliga befogenheterna kan inte utövas fullt ut utan tillräcklig erfarenhet samt utan kunnande och färdigheter. Särskild uppmärksamhet ska riktas på informationssäkerheten och behandlingen av personuppgifter.

Den som utför de uppgifter inom militär underrättelseinhämtning vilka avses i bestämmelsen får utöva de befogenheter som avses i denna lag endast under uppsikt och övervakning av en tjänsteman som tjänstgör för en militärunderrättelsemyndighet. Således innehas det primära ansvaret av den tjänsteman som handleder och övervakar den verksamhet som bedrivs av de personer som avses i bestämmelsen och som definierar uppgiften och en befogenhet som eventuellt ska utövas.

En i bestämmelsen avsedd person som fått tillräcklig utbildning kan för att utföra ett underrättelseuppdrag använda de metoder för underrättelseinhämtning som avses i 4 kap., med undantag för styrd användning av informationskällor, täckoperationer och bevisprovokation genom köp. Även om bestämmelsen i sig ger omfattande befogenheter, är tillräcklig utbildning och erfarenhet alltid en förutsättning för att utöva dessa. Den krets av personer som utövar befogenheterna avgränsas även av underrättelseverksamhetens hemliga natur, som styr till en noggrann prövning av vilka uppgifter och vilka metoder som ska stå till förfogande för den person som genomför uppdraget. Utbildningen, kunskaperna och kunnandet samt pålitligheten påverkar alltid bedömningen. De personer som avses i bestämmelsen får aldrig på egen hand bestämma vilka metoder för underrättelseinhämtning som kan användas och i vilken omfattning. Den militära organiseringen påverkar dessutom verksamheten.

De personer som avgått från en militärunderrättelsemyndighets tjänst utifrån 47 § i lagen om försvarsmakten och som är i en tjänst enligt värnpliktslagen eller som deltar i en frivillig övning enligt 18 och 19 § i lagen om frivilligt försvar kan använda alla metoder för underrättelseinhämtning som avses i 4 kap. under uppsikt och övervakning av militärunderrättelsemyndigheten. En ytterligare särskild förutsättning är att de är särskilt förtrodda med användningen av metoder för underrättelseinhämtning.

Det föreslås att paragrafens 2 mom. innehåller bestämmelser om befogenheterna vid en tjänst eller övning enligt 1 mom. för personer som avgått från en militärunderrättelsemyndighets tjänst.

Bestämmelsen gäller för de personer som uppnått avgångsåldern enligt 47 § i lagen om försvarsmakten. Exempelvis personer som uppnått avgångsåldern och som arbetat hos en militärunderrättelsemyndighet har i bästa fall flera decenniers erfarenhet och kunnande om militär underrättelseinhämtning. Dessutom kan de ha kunnande som de yngre generationerna inte ännu har. Således kan även personer enligt bestämmelsen vid behov användas för landets försvar och i skyddet av den nationella säkerheten.

Åldern för att avgå från Försvarsmaktens tjänsten har höjts under den senaste tiden. Det bör även observeras att den övre åldersgränsen för reservisterna har höjts till 65 levnadsår genom lag 1346/2025, som trätt i kraft den 1 januari 2026 genom en ändring av värnpliktslagen. På samma gång slopades den övre åldersgränsen för deltagarna i en frivillig övning inom landsförsvaret helt och hållet.

Kunnandet hos en person som deltar i en tjänst eller övning bedöms från fall till fall med hänsyn till personens erfarenhet.

Användningen av metoder för underrättelseinhämtning sker alltid under militärunderrättelsemyndighetens styrning och övervakning.

93 §. *Tjänsteansvar för den som inte arbetar i tjänsteförhållande.* Paragrafens rubrik ändras för att närmare beskriva personer som kan delta i militär underrättelseinhämtning. Den gällande bestämmelsen gäller endast personer i en tjänst enligt värnpliktslagen.

Enligt paragrafens 1 mom. utvidgas tjänsteansvaret att även gälla i föreslagna 91 § avsedda situationer enligt 18 och 19 § i lagen om frivilligt försvar. Tjänsteansvaret gäller även för andra än för värnpliktiga.

I paragrafens 2 mom. utvidgas tjänsteansvaret till att gälla även för andra än dem som står i ett tjänsteförhållande. Tjänsteansvaret är bredare än det ansvar som uppkommer utifrån ett anställningsförhållande. Vid förfarande i uppgifter som omfattar avsevärd offentlig makt, ska tjänsteansvaret täcka även personer med ett avtalsförhållande.

94 §. *Skadeståndsansvar för den som inte arbetar i tjänsteförhållande.* Paragrafens rubrik ändras för att motsvara de nya bestämmelserna. Bestämmelsen är informativ.

Paragrafens 1 mom. hänvisar till en person som då han eller hon vidtar en lagstadgad uppgift orsakar skada. Med person avses en annan person än en person som står i tjänsteförhållande, såsom en person i en tjänst enligt värnpliktslagen.

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 ett fartyg eller luftfartyg för krigsfolk. Det som nämns ovan innebär också en möjlighet till jämkning av skadestånd med beaktande av bland annat 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.

Bestämmelsen täcker även situationer där en person utanför militärunderrättelsemyndigheten ger bistånd för att installera eller avinstallera en anordning, metod eller ett program som förutsätts för att använda en metod för underrättelseinhämtning.

Enligt bestämmelserna i 3 kap. i skadeståndslagen är arbetsgivaren skyldig att ersätta en skada som en anställd genom ett fel eller en försummelse i sitt arbete orsakar tredje part (1 § 1 mom.). Om någon som på grund av förordnades av myndighet utför ett visst uppdrag som är fastställt genom lag utan att vara självständig företagare och genom fel eller försummelse vållar skada då han fullgör uppdraget, är den för vars räkning uppdraget utförs skyldig att ersätta skadan (1 § 3 mom.). Till exempel en beväring har ansetts vara en person som utför arbete i ett offentlighetsrättsligt rättsförhållande, för vilken en offentlig sammanslutning kan ställas inför skadeståndsansvar. Hänvisningarna till bestämmelserna i skadeståndslagen utvidgar med andra ord principalansvaret.

Det föreslås att 2 mom. i paragrafen innehåller bestämmelser om ersättningsansvaret för en person som deltar i en frivillig övning enligt 18 och 19 § i lagen om frivilligt försvar. Bestämmelserna om ersättningsansvaret för en beväring i 4 kap. i skadeståndslagen tillämpas på ersättningsansvaret. Bestämmelsen är materiell, eftersom skadeståndslagen inte innehåller bestämmelser om skadeståndsansvaret för personer som deltar i det frivilliga försvaret av landet. Bestämmelsen motsvarar vad som föreskrivs om skadeståndsansvar i lagen om frivilligt försvar.

96 §. *Biståndsskyldighet för kommunikationsförmedlare och leverantörer av datacentraltjänster.* I paragrafen föreslås en ändring enligt vilken det i bestämmelsen framöver hänvisas till kommunikationsförmedlare som avses i 3 § 36 punkten i lagen om tjänster inom elektronisk kommunikation i stället för till teleföretag och samfundsabonnenter. Med kommunikationsförmedlare avses en sådan annan aktör som förmedlar elektronisk kommunikation för andra än personliga eller med sådana jämförbara sedvanliga privata ändamål.

Dessutom gäller skyldigheten att ge bistånd även för leverantörer av datacentraltjänster. Datacentraltjänst har definierats i 2 § 2 punkten i cybersäkerhetslagen och avser en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll. Skyldigheten gäller en aktör som tillhandahåller ovan avsedda tjänst.

I paragrafens 1 mom. nämns även en ny metod för underrättelseinhämtning, underrättelseinhämtning i Finland som avser statliga aktörers datasystem. En kommunikationsförmedlare och leverantör av datacentraltjänster ska biträda en militärunderrättelsemyndighet på samma sätt som vid till exempel teleavlyssning.

Enligt paragrafens 2 mom. har militärunderrättelsemyndigheten och den som utför åtgärden och den biträdande personalen rätt att för att göra de kopplingar som behövs för teleavlyssning få tillträde också till andra utrymmen än de som är i kommunikationsförmedlaren eller leverantörens av informationssamhällets tjänster besittning, dock inte till utrymmen som används för stadigvarande boende. En med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman fattar beslut om åtgärden.

Momentet innehåller även en hänvisning till en leverantör av datacentraltjänster på samma sätt som man hänvisat till en leverantör av kommunikationstjänster.

97 §. *Dataöverförarens skyldighet att medverka till genomförandet och upprätthållandet av den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter.* Paragrafens 2 mom. ändras. I och med ändringen kan en militärunderrättelsemyndighet genomföra en accesspunkt som underrättelseinhämtning som avser datatrafik kräver utan medverkan av dataöverföraren, om det är nödvändigt för att skydda underrättelseinhämtningen. I praktiken hänför sig åtgärden till dataöverförare som inte är välvilligt inställda och som kan innehas av till exempel en aktör från en främmande stat.

Med termen underrättelseinhämtning som används i bestämmelsen hänvisar man allmänt till de underrättelsemyndigheter som använder underrättelseinhämtning som avser datatrafik, det vill säga en militärunderrättelsemyndighet och skyddspolisen. Militärunderrättelsemyndigheten fungerar som teknisk genomförare av underrättelseinhämtning som avser datatrafik för skyddspolisen. Ett av delområdena i det tekniska genomförandet är att genomföra en

accesspunkt, varför accesspunkten vid behov ska kunna genomföras i hemlighet i enlighet med skyddspolisens behov.

I praktiken har man observerat situationer där en dataöverförare som ska anses vara av ringa betydelse för kommunikationsnätets funktion kan administrera en viss del av ett kommunikationsnät. Dataöverföraren är dock en aktör som inte kan kontaktas eller så opererar aktören under styrning av en statlig aktör. Det är självklart att en accesspunkt inte kan genomföras utan medverkan av dataöverföraren i sådana situationer.

Det står klart uppbyggandet av en accesspunkt inte får orsaka någon onödig olägenhet för ett allmänt kommunikationsnät. Redan de allmänna principerna i lagen och risken för att verksamhetens ska avslöjas styr mot detta. Till exempel en central aktör för ett allmänt kommunikationsnät i Finland kan i praktiken aldrig vara föremål för de åtgärder som avses i bestämmelsen, eftersom åtgärderna kan orsaka avsevärd olägenhet, varvid militärunderrättelsemyndighetens verksamhet kan röjas.

En accesspunkt ska fortfarande i princip genomföras med dataöverförarens medverkan och i princip har dataöverföraren i situationer enligt 2 mom. rätt att i mån av möjlighet vara på plats då en accesspunkt genomförs. När en militärunderrättelsemyndighet i hemlighet genomför en accesspunkt, ska den alltid noggrant överväga åtgärdernas nödvändighet såväl operativt som juridiskt.

99 §. Ersättningar till kommunikationsförmedlare och leverantörer av datacentraltjänster. I paragrafen görs ändringar som beror på de ovan föreslagna motsvarande ändringarna i 97 § avseende ersättningsmottagarna.

101 §. Sökande av ändring i ett ersättningsbeslut. Paragrafen motsvarar i praktiken det som i den gällande lagen föreskrivs om sökande av ändring i ett ersättningsbeslut. I 1 mom. görs ändringar som beror på de föreslagna ändringarna i 97 §.

Paragrafens 2 mom. innehåller en informativ hänvisning till förvaltningslagen och lagen om rättegång i förvaltningsärenden i fråga om omprövning av beslut och rätten att överklaga.

Paragrafens 3 mom. motsvarar 4 mom. i den gällande paragrafen. Momentet innehåller bestämmelser om Transport- och kommunikationsverkets rätt att bli hört, om ett ersättningsärende handläggs i förvaltningsdomstolen.

104 §. Rätt att få information av privata sammanslutningar. Paragrafens 2 mom. ändras för att motsvara vad som föreskrivs annanstans till exempel om brottsbekämpning. Framöver kan föremålet för en begäran om information vara en leverantör av informationssamhällets tjänster i stället för en samfundsabonnent som nämns för närvarande i bestämmelsen. Med informationssamhällets tjänster avses i 3 § 29 punkten i lagen om tjänster inom elektronisk kommunikation avsedda informationssamhällets tjänster såsom elektroniska tjänster som utförs på individuell begäran av en mottagare, på distans och vanligtvis mot ersättning. Med tillhandahållare av informationssamhällets tjänster avses på motsvarande sätt en tillhandahållare av tjänster som tillhandahåller informationssamhällets tjänster som avses i 3 § 29 punkten i lagen om tjänster inom elektronisk kommunikation. Sådana tillhandahållare kan vara till exempel tillhandahållare av molntjänster eller olika datacentralstjänster eller andra tillhandahållare av digital infrastruktur, såsom internetbaserade marknadsplatser eller sökmotorer, eller olika plattformar för sociala nätverkstjänster.

Bakgrunden till de föreslagna ändringarna är förändringar i omvärlden, i synnerhet digitaliseringen av samhället och den därmed anslutna tekniska utvecklingen, till följd av vilka de gällande bestämmelserna inte längre till alla delar motsvarar de praktiska behoven. Den nya formuleringen täcker en bredare grupp av olika aktörer än tidigare och alla olika aktörer som deltar i tillhandahållandet av tjänster, från vilka en militärunderrättelsemyndighet kan få uppgifter för skötseln av de egna uppgifterna. I en servicekedja kan det ingå flera olika tillhandahållare av tjänster som har olika uppgifter och roll i tjänsteproduktionen, även om en tillhandahållare av tjänster inte i sig förmedlar kommunikationen.

De uppgifter utifrån vilka en begäran om information enligt bestämmelsen kan göras innehas redan av militärunderrättelsemyndigheten och de har inhämtats till exempel med en annan metod för underrättelseinhämtning. Föremålet för en begäran kan således vara till exempel vem som använde en viss IP-adress under viss tidpunkt. Syftet med bestämmelsen är inte att bryta en ända till ända-kryptering.

Dessutom ändras 2 mom. på så sätt att det tydligt redogör för att en militärunderrättelsemyndighet har rätt att få de uppgifter som behövs för att identifiera en tjänsts användare eller abonnent. Med användare avses enligt 3 § 7 punkten i lagen om tjänster inom elektronisk kommunikation en fysisk person som i egenskap av abonnent eller annars använder kommunikationstjänster eller mervärdestjänster. Med abonnent avses enligt 3 § 30 punkten i den lagen en juridisk eller fysisk person som för något annat ändamål än televerksamhet har ingått avtal om leverans av kommunikationstjänster eller mervärdestjänster. Med stöd av en begäran om information kan en militärunderrättelsemyndighet få sådana behövliga uppgifter med vilka det är möjligt att identifiera en användare eller abonnent.

Rätten att få information enligt paragrafen gäller även framöver uppgifter som behövs för att utföra ett underrättelseuppdrag.

Förvaltningsutskottet har i sitt betänkande FvUB 1/2024 rd samt i sina tidigare ställningstaganden (FvUU 37/2022 rd, FvUB 42/2022 rd, FvUB 3/2023 rd) ansett att det till exempel i fråga om hemliga metoder för inhämtande av information är motiverat att bestämmelserna revideras på ett enhetligt sätt och att innehållet i bestämmelserna är så lika som möjligt. Det är enligt utskottets uppfattning inte ändamålsenligt att det finns ogrundade skillnader i bestämmelser om i sak samma metoder. Exempelvis enhetliga bestämmelser om hemliga metoder för inhämtande av information är viktiga med tanke på ett fungerande myndighetssamarbete. Tydliga och konsekventa bestämmelser ökar inte bara effektiviteten i behandlingen utan också likabehandlingen av objekten. På motsvarande sätt ska det beaktas att regleringen är av samma innehåll även i fråga om de olika myndigheternas rätt att få information och under vissa förutsättningar även för rättigheterna att dela och förmedla mottagen information till andra myndigheter.

I fråga om ändringarna i paragrafens 2 mom. handlar det inte om en situation där de företag eller sammanslutningar som erbjuder tjänster måste avstå från en ända till ända-kryptering eller att underlätta eller möjliggöra att militärunderrättelsemyndighetens får allmänt tillträde till deras system eller tjänster.

Ett nytt 3 mom. fogas till paragrafen. I momentet föreskrivs uttryckligen att uppgifterna kan fås utan dröjsmål och avgiftsfritt, om inte något annat föreskrivs i lag.

111 §. Undersökning av upptagningar. Paragrafens 1 mom. ändras. Enligt den gällande regleringen får upptagningar som samlats in genom att använda metoderna för underrättelseinhämtning undersökas bland annat av en med användningen av metoder för

underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman, vilken förordnats till uppgiften hos militärunderrättelsemyndigheten. För tydlighetens skull ändras momentet till denna del på så sätt att upptagningar får undersökas av en tjänsteman som förordnats till uppdraget av militärunderrättelsemyndigheten, vilket bättre motsvarar verksamheten i praktiken hos militärunderrättelsemyndigheten.

I den gällande bestämmelsen kan ett beslut om de personer som har rätt att undersöka upptagningar hos militärunderrättelsemyndigheten fattas endast av huvudstabens underrättelsechef. I praktiken har det konstaterats att nivån för beslutsfattandet är för hög och även en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman ska kunna fatta motsvarande beslut. I och med den föreslagna ändringen kan ett beslut med andra ord fattas av tjänstemän som befinner sig närmare den praktiska verksamheten, vilka är insatta i den aktuella uppgiften, och nivån på beslutsfattandet motsvarar bättre vad som är fallet i fråga om exempelvis beslut om utövning av metoder för underrättelseinhämtning. Till denna del motsvarar bestämmelsen vad som föreskrivs om undersökning av upptagningar i 5 a kap. i polislagen.

Till övriga delar görs inga ändringar i paragrafen.

7.2 Lagen om försvarsmakten

8 b §. *Inhämtande av information från allmänt tillgängliga källor.* Paragrafen är ny. Paragrafen innehåller bestämmelser om Försvarsmaktens rätt att inhämta information från allmänt tillgängliga källor. Således kan information inhämtas av en militärunderrättelsemyndighet och därtill exempelvis av Försvarsmaktens forskningsinstitut och de aktörer som ansvarar för Försvarsmaktens cyberförsvar.

Med allmänt tillgängliga källor avses utöver sedvanliga öppna källor, såsom dagstidningar och sedvanliga nyhetstjänster, även digitala tjänster, som kan förutsätta att man loggar in eller skapar en profil i dessa. Sådana digitala tjänster utgörs av bland annat sociala medier (Facebook och TikTok) och informationstjänster som kräver registrering, såsom Jane's Information Service. Uttryckligen registrering, skapande av en annan motsvarande profil eller utlämnande av uppgifter skulle vara en central skillnad jämfört med underrättelseinhämtning som avser sedvanliga öppna källor. Då man av tradition ansett att information från öppna källor är tillgänglig för vem som helst utan utlämnande av information, kan det vara nödvändigt att lämna vissa uppgifter i allmänt tillgängliga källor. Ovan nämnda informationskällor kan kallas för en begränsad öppen informationskälla.

Definitionen av allmänt tillgängliga öppna källor är dock relativt bred och den ska alltid bedömas i förhållande till vad som varit avsikten för den aktör som ställt uppgifterna till förfogande, till exempel att få så stor synlighet som möjligt för uppgifterna eller om aktören noggrant kontrollerar tillträdet till uppgifterna. Till exempel förutsätter många informationstjänster registrering, men vem som registreras kontrolleras inte nödvändigtvis på något sätt och registreringen godkänns automatiskt.

Å andra sidan är syftet i vissa digitala tjänster uttryckligen att förebygga att användaren identifieras, såsom i nätet Tor. I dessa tjänster kan det även förmodas att det finns informationsmaterial som är väsentligt med tanke på Försvarsmaktens uppgifter. Det är även möjligt att tjänsterna används för att läcka information, vilket kan ge till och med betydelsefull information för till exempel den militära underrättelseinhämtningen.

Huruvida till exempel en grupp inom sociala medier kan anses vara en sådan allmänt tillgänglig källa som avses i bestämmelsen beror på den förhandenvarande situationen. I rättslitteraturen har man som ett grovt exempel för gränsdragningen hänvisat till att om ett meddelande är riktat endast till kompisar eller delar av dem, bildar de inte ännu en publik, under förutsättning att det finns endast några kompisar. Om kompiskretsen är stor, till exempel hundratals personer, bildar gruppen redan en publik. Utgångspunkten ska anses utgöras av huruvida medlemmarna i gruppen kan anses utgöra en tät vänskrets eller om det handlar om en helhet där medlemmarna inte har någon tät social relation som omfattar alla medlemmar i gruppen. Om gruppen handlar endast om en tät kompisgrupp, ska medlemskapet i gruppen upphävas eller alternativt ska ett konto på sociala medier överföras till exempel till militärunderrättelsemyndigheten, så att den vid behov kan inhämta information genom metoderna för underrättelseinhämtning.

Information som inhämtats från allmänt tillgängliga källor är allmän information som är tillgänglig från källor. Vid inhämtning av information enligt bestämmelsen är informationsproducenten eller den som skickat ett meddelande inte av betydelse, endast den information som ingår i meddelandet. Om man till exempel börjar följa en viss person eller gruppmedlem på en plattform på sociala medier, handlar det inte nödvändigtvis längre om information som skaffas från öppna källor, utan till exempel om systematisk observation som föreskrivs som en befogenhet för en militärunderrättelsemyndighet eller en brottsbekämpningsmyndighet. I situationen påverkas bedömningen dock av om det handlar om en offentlig person och i vilken roll personen deltar i diskussionen eller uppdateringar.

Således handlar underrättelseinhämtning enligt bestämmelsen i princip alltid om innehållet och om att följa innehållet. I och med att innehållet följs är det dock möjligt att vissa aktörer återkommer som dataproducenter, men i detta fall har själva inhämtandet av information inte skett utifrån dataproducenten.

Vid inhämtning av information enligt paragrafen är det möjligt att ett behov av att lagra personuppgifter uppkommer. Vid lagring och behandling ska lagen om behandling av personuppgifter inom Försvarsmakten iakttas.

I paragrafens 1 mom. föreskrivs en befogenhet för Försvarsmakten att inhämta och behandla information från allmänt tillgängliga källor. Inhämtandet av information ska dock hänföra sig till Försvarsmaktens uppgifter, varför det inte kan hänföras till vilken information som helst.

Paragrafens 2 mom. innehåller bestämmelser om rätten att använda tekniska metoder då inhämtande av information enligt 1 mom. genomförs. Bestämmelsen avgränsar inte metoderna för inhämtande av information, utan information kan inhämtas även på automatiserat sätt. Således kan inhämtandet av information ske genom att en enskild tjänsteman bläddrar i en tidning eller med datatekniska metoder genom att använda en algoritm. På motsvarande sätt kan informationen lagras genom att använda en kopieringsmaskin eller lagra den i en dators hårddisk genom att använda en programvara i datorn.

I paragrafens 3 mom. regleras skydd av inhämtande av information från allmänt tillgängliga källor, det vill säga användning av så kallade lätta täckidentiteter. Behovet av sådana täckidentiteter i Försvarsmaktens övriga verksamhet än den militära underrättelseverksamheten anknyter till att Försvarsmaktens verksamhet inte ska avslöjas i samband med ett eventuellt dataintrång. Till exempel Försvarsmaktens forskningsverksamhet kan äventyras om en aktör som orsakar ett hot för landets försvar får information om målen för Försvarsmaktens forskningsverksamhet.

I det fall som avses i bestämmelsen handlar det om att påhittade uppgifter ges i samband med registrering eller skapande av en profil. I skyddet enligt bestämmelsen ska man rikta uppmärksamhet på hur pålitlig registrering eller profil som förutsätts i tjänsten. Om man för att registrera sig till exempel i ett diskussionsforum förutsätter endast namn och vissa adressuppgifter och att man hittar på en pseudonym, och uppgifterna inte granskas desto närmare, handlar det om sådant skydd som avses i bestämmelsen. Om registreringen å sin sida förutsätter lämnande av betalningsinformation och stark identifiering med bankkoder, handlar det inte längre om i bestämmelsen avsett skydd av inhämtande av information från allmänt tillgängliga källor.

Det kan till exempel vara nödvändigt att skapa en e-postadress för en lätt täckidentitet som används vid registrering. Detta kan vara av betydelse för registreringen och därtill för administreringen av ett användarnamn eller en profil. Samma principer som i anknytning till ovan beskrivna tjänster gäller för skapande av en e-postadress. En e-postadress får inte användas för annat än för att skapa en lätt täckidentitet och ta emot meddelanden i anknytning till det. Via e-post är det inte möjligt att föra en diskussion med en annan person, eller om detta är fallet, ska diskussionen avslutas utan oskäligt dröjsmål.

Det står klart att det inte är tillåtet att inleda direkt umgänge vid anskaffning av information från allmänt tillgängliga källor med andra personer till exempel i ett diskussionsforum eller i en grupp på sociala medier. Diskussionen och deltagandet i diskussionen kan i regel anses handla om förtäckt inhämtande av information i brottsbekämpning och underrättelseinhämtning. Dock kan det uppstå situationer där det krävs aktivitet för att hållas kvar i ett diskussionsforum eller i en grupp. I så fall ska kommunikationen föras på allmän nivå och den får inte leda till längre kommunikation med en annan medlem i gruppen.

Det är ändamålsenligt att ordna det skydd som avses i bestämmelsen på så sätt att man så långt som möjligt använder permanenta lätta täckidentiteter, vars användare dock kan bytas enligt situationen. Detta bidrar till att underlätta laglighetsövervakningen av verksamheten och organiseringen av användningen av lätta täckmantlar.

Det finns till exempel många olika former av grupper på sociala medier. Grovt sett kan man tala om offentliga, slutna och hemliga grupper. Vem som helst kan ansluta sig till den första av dessa utan desto mer invecklade processer för att få tillträde till gruppen.

I slutna grupper förutsätts ett godkännande för att få tillträde till gruppen. Med tanke på den nu behandlade bestämmelsen innebär detta att om en förutsättning för att få tillträde till gruppen endast är att en begäran framförs, är gruppen tydligt en sådan offentligt tillgänglig källa som avses i bestämmelsen. Om tillträdet till en grupp inte förutsätter att man svarar på detaljerade frågor om personen själv, närmar sig verksamheten redan användning av metoder för underrättelseinhämtning, varvid tillträdet till gruppen inte längre kan anses vara inhämtande av information från allmänt tillgängliga källor. Å andra sidan, om en förutsättning för att få tillträde till en grupp är att svara på en allmän enkät till exempel i fråga om en åsikt om ett visst ärende, handlar det om inhämtande av information enligt paragrafen och användning av en lätt täckidentitet.

Som en tredje typ av grupp kan man nämna sådana grupper som inte syns allmänt för användarna och som i regel förutsätter en inbjudan till gruppen av en administratör. Vid en inbjudan till en sådan grupp, är det möjligt att ansluta sig till den. Det är dock inte tillåtet att påbörja umgänge med gruppens administratör eller avsändaren av inbjudan. I praktiken handlar denna situation om godkännande av en inbjudan med tanke på den verksamhet som avses i paragrafen. Dock kan förutsättningen för att få tillträde till en hemlig grupp vara att svara på

frågor, vilket kan göras inom ramen för en lätt täckidentitet, men svaren ska ges på allmän nivå och de får inte leda till umgänge med administratören eller gruppmedlemmarna.

Vissa tekniska metoder för att skydda Försvarmaktens datatrafik och dataskydd, såsom VPN-tjänster, betraktas inte som sådant skydd som avses i bestämmelsen.

Enligt paragrafens 4 mom. fattar huvudstaben beslut om de förvaltningsenheter inom Försvarmakten som ska ha rätt att använda det skydd för det inhämtande av information som avses i 3 mom. Alla förvaltningsenheter vid Försvarmakten har ett behov av att inhämta information från allmänt tillgängliga källor, och bestämmelsen hindrar inte detta. Alla förvaltningsenheter vid Försvarmakten har dock inte något behov av att använda skydd vid inhämtandet av information, varför dessa förvaltningsenheter kan fastställas närmare genom beslut av huvudstaben. Förvaltningsenheterna enligt beslutet ska ha ett befogat behov av att skydda sin verksamhet. Till exempel kan det bedömas att alla enheter som tillhandahåller beväringutbildning inte har något behov av att skydda inhämtandet av information från allmänt tillgängliga källor.

Det centrala är att användningen av skyddet är centraliserat till vissa förvaltningsenheter hos Försvarmakten.

Paragrafens 5 mom. innehåller bestämmelser om den tjänsteman som ansvarar för användningen av skydd, vilken i ett beslut enligt 4 mom. är chefen för Försvarmaktens förvaltningsenhet. Chefen ansvarar även för användningen av skydd i sin förvaltningsenhet. Lagenligheten i de åtgärder som avses generellt i paragrafen övervakas som en del av Försvarmaktens laglighetsövervakning.

8 c *Utplåning av uppgifter som inhämtats från allmänt tillgängliga källor.* Det föreslås att paragrafen innehåller bestämmelser om granskning av upptagningar och handlingar vilka fåtts under tiden för inhämtande av information enligt 8 b § och om utplåning av uppgifter. För tydlighetens skull konstateras i 1 mom. en huvudregel för informationsbehandling, enligt vilken en myndighet utan dröjsmål ska utplåna sådana uppgifter som inte behövs för att utföra uppdrag.

Paragrafens 2 mom. innehåller enligt förslaget en informativ hänvisning till lagen om behandling av personuppgifter inom Försvarmakten.

36 a §. Ledigförklarande av tjänster. Ett nytt 3 mom. fogas till paragrafen. I paragrafens 3 mom. föreskrivs att när en annan tjänst eller ett annat tjänsteförhållande enligt 1 eller 2 mom. tillsätts genom ett ansökningsförfarande, kan Försvarmakten låta bli att meddela dem som sökt tjänsten eller tjänsteförhållandet och namnen på de andra sökandena och namnet på den som har utnämnts, om uppgiftens art nödvändigt kräver det. Med nödvändighet avses att detta är ett sistahandsalternativ, varvid Försvarmakten i samband med att en tjänst tillsätts ska pröva sättet att tillsätta en tjänst eller ett tjänsteförhållande med tanke på ämbetsverkets personal- och organisationssäkerhet, hoten i anknytning till uppgifterna, skyddet av militär underrättelseinhämtning eller ett annat synnerligen viktigt allmänt eller privat intresse och väga om förutsättningen om nödvändighet är uppfylld. Utgångspunkten är att ett öppet ansökningsförfarande fortfarande ska vara huvudregeln, medan tillsättning av tjänster och tjänsteförhållanden utan att de ledigförklaras ska vara ett undantagsförfarande.

Vissa tjänster vid Försvarmakten har en särskild karaktär som omfattar specialkunnande inom landsförsvar, skydd av den nationella säkerheten, militär underrättelseinhämtning samt hemliga metoder för underrättelseinhämtning inom brottsbekämpning och hemliga tvångsmedel.

Beroende på arten av en tjänstemans uppgift ska identiteten skyddas effektivt och hållas sekretessbelagd från första början.

Till exempel centrala uppgifter som gäller militär underrättelseinhämtning, där en tjänstemans identitet ska skyddas effektivt redan i rekryteringsskedet, har en koppling till operativa uppdrag inom militär underrättelseinhämtning och andra stöduppgifter samt analysuppgifter som gäller uppgifterna. I den operativa verksamheten är det till exempel med tanke på skyddet av informationskällor av primär vikt att en informationskälla inte kan identifieras via en tjänsteman inom militär underrättelseinhämtning. Till exempel stöduppgifterna för den operativa verksamheten vid militär underrättelseinhämtning omfattar bland annat operativa uppgifter som sköts av jurister och operationsrelaterade uppgifter som anknyter till teknik-, ekonomi- och personalförvaltningen.

Ett centralt element i den helhet som utgörs av Försvarmaktens verksamhet är tillgången till information i en tjänst eller ett tjänsteförhållande och att informationen anhopas. De tjänstemän som utför Försvarmaktens uppdrag och som innehar information kan vara föremål för inhämtande av information och försök till påverkan av främmande stater. Tjänsteman ska skyddas mot påtryckningar, utpressning, hot om våld och rekryteringsförsök. Om en tjänstemans identitet röjs, innebär det att tjänstemannen inte kan sköta uppgifterna på grund av risk för rekryteringsförsök, fara för liv eller hälsa eller för att hans eller hennes förmåga att utföra uppgifterna har äventyrats. Identitetsskyddet av dem som sköter förvaltnings- och teknologiuppgifter vid Försvarmakten bedöms på samma grunder som identitetsskyddet av dem som arbetar med operativa uppdrag eller analysuppdrag inom militär underrättelseinhämtning.

Vid bedömningen av nödvändigheten enligt 3 mom. ska man beakta Försvarmaktens personal- och organisationssäkerhet, den uppgift som ska tillsättas samt de anknutna hoten samt ett annat synnerligen viktigt allmänt eller privat intresse.

Information om tillsättandet av en tjänst eller ett tjänsteförhållande ska ges till sökandena genom att överlämna utnämningsbeslutet för kännedom. I så fall ska den tjänst eller det tjänsteförhållande som ledigförklarats, den beslutsfattande myndigheten och utnämningsdatum uppges. Genom förfarandet tryggas möjligheten att utnyttja rätten att söka ändring. Tryggandet av rätten att söka ändring i ett beslut som gäller utnämning till en tjänst innebär att utnämningsbeslutet kan ändras i efterhand till följd av besvär, vilket bidrar till att främja jämställdheten samt likabehandlingen av sökandena. När det gäller det offentliga ansökningsförfarandet kan man inte utesluta möjligheten att det bland sökandena finns statliga aktörer som döljer sin verksamhet. Då finns det en risk för att uppgifter om de andra sökandena eller om den valda personen sprids.

När Försvarmaktens tjänster eller tjänsteförhållanden tillsätts är en öppen tjänsteansökan fortfarande utgångspunkten.

Bestämmelsen påverkar inte tillämpningen av offentlighetslagen. Varje begäran om information ska bedömas enligt offentlighetslagen.

7.3 Strafflagen

7 §. Riksgränsbrott. Enligt paragrafens 2 mom. döms för riksgränsbrott inte en utlänning som gjort sig skyldig till ett riksgränsbrott utifrån 78 § 5 mom. i lagen om militär underrättelseverksamhet. Det handlar om en situation där en person som hjälpt Finland utsätts för fara som gäller liv eller hälsa i sitt avgångsland och det är nödvändigt att få personen ut ur

sitt avgångsland för att skydda personens liv och hälsa. I situationerna finns det på grund av rimlighetsskäl och för klarhetens skull skäl att utfärda separata bestämmelser om åtalsfrihet som gäller riksgränsbrott.

Genom att till ovan hänvisade delar slopa gärningens straffbarhet, gör sig en person inte skyldig till en gärning enligt 17 kap. 7 § i strafflagen genom att använda falska handlingar som militärunderrättelsemyndigheten gett honom eller henne utifrån 78 § 5 mom. i lagen om militär underrättelseverksamhet. Å andra sidan är det möjligt att det på grund av ärendets känsliga karaktär är nödvändigt att ordna en person över Finlands gräns på annat sätt än via ett officiellt gränsövergångsställe.

I dessa situationer är det möjligt att personen blir kvar i Finland, vilket förutsätter normala invandringsprocesser eller en asylansökan, men i situationerna kan Finland även vara endast ett transitland, varifrån personer överförs till en tredje stat.

7.4 Lagen om Finansinspektionen

71 d §. Rätt att lämna ut uppgifter till skyddspolisen och militärunderrättelsemyndigheterna. En hänvisning till militärunderrättelsemyndigheterna fogas till paragrafens 1 mom. I och med tillägget har militärunderrättelsemyndigheterna inom sitt område motsvarande rätt att få uppgifter från Finansinspektionen som skyddspolisen inom det egna området.

Enligt bestämmelsen har Finansinspektionen rätt att trots sekretessbestämmelserna på begäran lämna ut uppgifter till militärunderrättelsemyndigheterna, om uppgifterna är nödvändiga för ett underrättelseuppdrag. Enligt 10 § 9 punkten i lagen om militär underrättelseverksamhet avses med 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 14 §.

I den föreslagna bestämmelsen kan de uppgiftsinnehåll ska lämnas ut inte räknas upp på övergripande sätt, varför utlämnandet av uppgifterna är bundet till nödvändighetskriteriet.

Till paragrafens 2 mom. fogas en motsvarande ändring, enligt vilken Finansinspektionen har rätt att utan hinder av sekretessbestämmelserna på eget initiativ till militärunderrättelsemyndigheten lämna ut information som Finansinspektionen har i sin besittning gällande penningtvätt eller finansiering av terrorism, kringgående av sanktionsbestämmelser eller andra ovanliga transaktioner genom vilka medel överförs till tredjeländer då åtgärderna misstänks ha en koppling till militär verksamhet eller äventyra den nationella säkerheten, om informationen är behövlig för militär verksamhet som hör till militärunderrättelsemyndighetens verksamhetsområde och för skyddande av den nationella säkerheten mot verksamhet som allvarligt hotar den.

Dessutom föreslås att man på utlämnande av uppgifter enligt 1 och 2 mom. i paragrafen tillämpar 71 § 5 mom. i lagen, vilket innehåller bestämmelser om de situationer där Finansinspektionen inte får lämna ut uppgifter, om den inte fått samtycke till att uppgifterna lämnas ut.

7.5 Lagen om Enheten för utredning av grå ekonomi

6 §. *Syftet med fullgöranderapporter.* Paragrafens 39 punkt ändras genom att byta punkten till ett kommatecken.

En ny 40 punkt fogas till paragrafen. Enligt den kan fullgöranderapporter utarbetas till stöd för militär underrättelseinhämtning enligt lagen om militär underrättelseverksamhet. Den föreslagna ändringen gäller rapporter som ska ges om syftet med militär underrättelseinhämtning enligt 3 § i lagen om militär underrättelseverksamhet. Den föreslagna ändringen om en ny 40 punkt möjliggör framöver att fullgöranderapporter utarbetas till stöd för militärunderrättelsemyndigheternas verksamhet. Militär hot och hot mot den nationella säkerheten kan i sig anses vara så allvarliga att fullgöranderapporter ska kunna utarbetas för att främja skötseln av militärunderrättelsemyndighetens uppgifter.

Enligt 7 § i lagen om Enheten för utredning av grå ekonomi har utredningsenheten rätt att trots sekretess av myndigheterna få de uppgifter som är nödvändiga för utarbetandet av en fullgöranderapport och som den myndighet som begär rapporten har rätt att få för det ändamål som uppges i begäran. Rätten att få information för militärunderrättelsemyndigheten som en del av Försvarsmakten föreskrivs i 17 § i lagen om försvarsmakten. Enligt bestämmelsen har Försvarsmakten rätt att trots sekretessplikten av myndigheter och av sammanslutningar som tillsatts för att sköta ett offentligt uppdrag få de uppgifter och handlingar som är nödvändiga för skötseln av lagstadgade uppdrag, om inte lämnandet av uppgiften eller handlingen till Försvarsmakten eller användningen av uppgifterna som bevis har förbjudits eller begränsats i lag.

Då den reglering som tillämpas på de informationsmässiga befogenheterna för uppgifterna för en militärunderrättelsemyndighet och skyddet av den nationella regleringen är utspridd över flera bestämmelser, är det i praktiken väldigt svårt att precisera regleringen på en gång. En militärunderrättelsemyndighets uppgifter och skyddet av den nationella säkerheten är i sig en relativt vag grund för erhållande av information för en civil- och militärunderrättelsemyndighet, varför det är motiverat att koppla grunden till erhållande av uppgifter fastare till civil- och militärunderrättelseverksamhetens syfte och de objekt för civil och militär underrättelseinhämtning som fastställts i underrättelselagarna. På grund av detta är det motiverat att bestämmelserna om informationsmässiga befogenheter för militärunderrättelsemyndigheten kopplas till hotande verksamhet enligt 4 § i lagen om militär underrättelseverksamhet då en sådan koppling kommer fram av någon annan kontext. I fråga om de informationsmässiga befogenheter som föreskrivs i lagen om militär underrättelseverksamhet kan kopplingen, med beaktande av 17 § i lagen om försvarsmakten, anses framgå av kontexten och i 104 § i lagen om militär underrättelseverksamhet har kopplingen konstaterats även uttryckligen.

Vid användning av ett underrättelseuppdrag inom militär underrättelseinhämtning som grund för att lämna ut uppgifter förutsätts således att regleringen är detaljerad och kravet på ändamålsenlighet och behövlighet i anknytning till skyddet för personuppgifter är uppfyllda. De föremål som räknas upp i 4 § i lagen om militär underrättelseverksamhet är av militär natur, varvid ett hot alltid anses vara allvarligt eller ett hot som allvarligt äventyrar den nationella säkerheten.

Syftet med fullgöranderapporterna är att ge en korrekt och tillräcklig helhetsbild av en organisation och dess skötsel av de offentlighetsrättsliga skyldigheterna utifrån information som finns i myndigheternas register. I fullgöranderapporterna beskrivs även organisationens direkta och indirekta kopplingar till andra organisationer eller organisationsanknutna personer. Det är ytterst viktigt att få en aktuell och heltäckande samlad bild av organisationen när sådana

ekonomiska aktörers bakgrund utreds som misstänks ha anknytning till verksamhet som äventyrar den nationella säkerheten. Fullgöranderapporterna är också viktiga vid utredningen av företagsomstruktureringar som misstänks anknyta till en främmande stats påverkansverksamhet.

7.6 Inkomstskattelagen

92 b §. *Vittnesarvode, belöning för tips och arvode som betalas för användning av informationskälla.* Det finns bestämmelser om skatteplikten för inkomst för en fysisk person i inkomstskattelagen. Den finländska skattesystemet baserar sig på ett brett inkomstbegrepp, enligt vilket den skattskyldiges inkomster i pengar eller pengars värde är skattepliktig inkomst, om det inte särskilt föreskrivs att de är skattefria.

I paragrafens 3 punkt föreskrivs att skattepliktig inkomst inte är arvode som en myndighet betalar en i lagen om militär underrättelseverksamhet (590/2019) och i polislagen (872/2011) avsedd informationskälla för inhämtande av uppgifter som är av betydelse för skötseln av ett underrättelseuppdrag eller för biträdande av en underrättelsemyndighet samt en i lagen om brottsbekämpning inom Gränsbevakningsväsendet (108/2018) avsedd informationskälla för inhämtande av uppgifter som är av betydelse för skötseln av uppdrag som hänför sig till upprätthållandet av gränssäkerheten.

Till punkten fogas en person som biträtt underrättelsemyndigheterna som en ny mottagare av skattefria arvoden. I situationerna handlar det om till exempel bistånd enligt föreslagna 42 § 2 mom. i lagen om militär underrättelseverksamhet. Det är viktigt att identiteten hos den som gett bistånd för de ifrågavarande åtgärderna inte avslöjas i samband med beskattningen. Det som även talar för arvodets skattefrihet är att arvoden som betalas till en biträdande personer är relativt sporadiska och små.

7.7 Gränsbevakningslagen

3 §. *Gränsbevakningsväsendets uppgifter.* Till paragrafens 3 mom. fogas en bestämmelse om Gränsbevakningsväsendets deltagande i militär underrättelseverksamhet. Det föreslås att föreslagna 25 a § och föreslagna 18 a § om befogenheterna i lagen om militär underrättelseverksamhet innehåller närmare bestämmelser om Gränsbevakningsväsendets deltagande i militär underrättelseinhämtning.

25 a §. *Gränsbevakningsväsendets deltagande i militär underrättelseinhämtning.* Paragrafen är ny. Paragrafen innehåller bestämmelser om Gränsbevakningsväsendets deltagande i militär underrättelseinhämtning.

I paragrafens 1 mom. föreskrivs att Gränsbevakningsväsendet på begäran deltar i militär underrättelseinhämtning genom att inhämta information och genom att vidta åtgärder till stöd för militärunderrättelsemyndigheternas underrättelseuppdrag. Uppgiften är ny för Gränsbevakningsväsendet.

Enligt 3 § i lagen om militär underrättelseverksamhet är syftet med militär underrättelseverksamhet att till stöd för den högsta statsledningens beslutsfattande och för de uppgifter för Försvarsmakten vilka separat räknats upp i paragrafen inhämta och behandla information om militär verksamhet som riktar sig mot Finland eller som är av betydelse med tanke på Finlands säkerhetsmiljö eller om någon annan verksamhet som allvarligt hotar det finska försvaret eller som äventyrar samhällets vitala funktioner.

Gränsbevakningsväsendet deltar i militär underrättelseinhämtning genom att stödja militärunderrättelsemyndigheten på begäran av denna i utförandet av en enskild åtgärd som gäller ett underrättelseuppdrag. Enligt definitionsbestämmelsen i 10 § 9 punkten i lagen om militär underrättelseverksamhet avses med underrättelseuppdrag ett uppdrag som huvudstabens underrättelsechef ger en militärunderrättelsemyndighet för att inhämta underrättelseinformation om ett 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 dessa. Avsikten med regleringen är inte att ändra ställningen för de nuvarande underrättelsemyndigheterna och Gränsbevakningsväsendet är i sitt uppdrag inte en militärunderrättelsemyndighet. Det handlar om utförande av kortvariga, enskilda uppdrag eller åtgärder i anknytning till ett underrättelseuppdrag och de sker alltid på begäran av militärunderrättelsemyndigheten. I vissa situationer kan begäran ha gjorts i förväg eller så kan den i situationer som kräver snabba reaktioner ske via jourarrangemang mellan myndigheterna.

Paragrafens 2 mom. innehåller en informativ hänvisning till att lagen om militär underrättelseverksamhet innehåller bestämmelser om Gränsbevakningsväsendets befogenheter för att delta i militär underrättelseinhämtning.

7.8 Lagen om behandling av personuppgifter vid Gränsbevakningsväsendet

32 §. *Utlämnande av personuppgifter till en annan behörig myndighet som avses i dataskyddslagen avseende brottmål.* Till paragrafens fogas ett nytt 2 mom. med bestämmelser om utlämnande av uppgifter om radioteknisk övervakning trots sekretessbestämmelserna för de uppgifter som föreskrivits för Försvarsmakten i lagen om militär underrättelseverksamhet. Det handlar om personuppgifter och andra uppgifter, vilka Gränsbevakningsväsendet enligt 15 b § i lagen behandlar för att genomföra radioteknisk övervakning under de förutsättningar som föreskrivits i 29 a–29 c § i gränsbevakningslagen. Enligt 29 a § 1 mom. i gränsbevakningslagen avses med radioteknisk övervakning att med hjälp av någon annan teknisk anordning än radar observera, identifiera, lokalisera, specificera och följa radiofrekventa elektromagnetiska vågor och radioutrustning med hjälp av egenskaperna hos de elektromagnetiska vågorna. Gränsbevakningslagen 29 b § innehåller bestämmelser om behandling av uppgifter från elektronisk kommunikation vid radioteknisk övervakning, medan 29 c § innehåller bestämmelser om behandling och utplåning av information från radioteknisk övervakning.

7.9 Lagen om behandling av personuppgifter inom Försvarsmakten

37 a §. *Militärunderrättelsemyndighetens rätt att upprätthålla sitt personregister.* Paragrafen är ny. Syftet med bestämmelserna är att främja dataskyddet och säkerställa att de uppgifter som militärunderrättelsemyndigheter lagrat i registret är korrekta och uppdaterade. Eftersom militärunderrättelsemyndighetens personregister innehåller uppgifter som ska behandlas för landets försvar och skyddet av den nationella säkerheten, är det föremål för särskilda datasäkerhetsrisker och dataskyddsrisker och ett synnerligen allvarligt hot om olaglig underrättelseverksamhet. För att hantera dessa har registret klassificerats på en hög informationssäkerhetsnivå och på grund av detta har systemet inga automatiserade kontakter utåt. Av denna orsak kan uppdateringen av uppgifterna inte heller göras på samma sätt som i system med en lägre informationssäkerhetsnivå, där uppgifterna kan uppdateras genom direkta förfrågningar om registrerade personer. Ett centralt krav är att det till ett register med lägre informationssäkerhetsnivå inte överförs uppgifter från ett register med högre informationssäkerhetsnivå i samband med en förfrågan. På grund av detta ska uppdateringen av informationen i ett register med hög dataskydds nivå genomföras på så sätt att ingen loggset eller annat dataset bildas avseende vilka uppgifter som uppdaterats i

militärunderrättelsemyndighetens personregister. Om föremålen eller intressena för militärunderrättelsemyndighetens underrättelseinhämtning avslöjas för utomstående eller objekten själva, kan detta äventyra landets försvar eller den nationella säkerheten.

De föreslagna bestämmelserna kan inte anses särskilt betydelsefulla med tanke på integritetsskyddet, eftersom möjliggörandet av jämförelsen inte utvidgar det uppgiftsinnehåll till vilket militärunderrättelsemyndigheten redan för närvarande har rätt. Bestämmelsen förtydligar lagstiftningen och gör den noggrannare avgränsad till den del som militärunderrättelsemyndigheten genom en teknisk förbindelse eller som ett dataset har rätt att få behövliga personuppgifter för att utföra sina uppdrag och för att administrera sina register. Bestämmelsen ändrar inte på det rådande rättsläget, men beaktar de krav som den tekniska utvecklingen ställer på dataskyddet och registrets korrekthet.

I paragrafens 1 mom. kopplas rätten att göra en jämförelse till de lagstadgade rätterna att få och lämna ut information. För tydlighetens skull konstateras i bestämmelsen att militärunderrättelsemyndigheten har rätt att få uppgifter för att utföra sina uppgifter trots sekretessbestämmelserna. Ett större dataset som samlats in från ett överlåtande register jämförs i den automatiska behandlingen med personuppgifterna i militärunderrättelsemyndighetens register. Personregistren står inte i direkt kontakt med varandra, utan de jämförs på en särskild teknisk plattform. Från fall till fall bedöms vad som är ett tillräckligt dataset för jämförelsen. Den kan gälla till exempel ändrade uppgifter, ett visst urvalsförfarande eller hela registerinnehållet. Vid tolkningen och tillämpningen av bestämmelsen ska de grundläggande principerna för behandling av personuppgifter i enskilda fall alltid beaktas.

Innan överföringen av uppgifterna inleds ska det utredas hur man ur olika register och datasystem tekniskt kan hämta ut de jämförelseuppgifter och övriga uppgifter som behövs och sammanställa dem i elektronisk form så att datainnehållet uppfyller jämförelsebehovet, och att hämtningen och sammanställningen av uppgifterna inte orsakar onödigt extra arbete och kostnader för den aktör som lämnar ut uppgifterna. Samtidigt minimeras behovet av extra behandling av uppgifterna.

I 1 mom. regleras också om skyldigheten att utplåna onödiga uppgifter. Efter analysen och behandlingen av jämförelseuppgifterna ska onödiga jämförelseuppgifter raderas utan dröjsmål från militärunderrättelsemyndighetens informationsresurs. I praktiken jämförs uppgifterna i en informationssäker miljö och sedan förstörs de uppgifter som har visat sig vara onödiga omedelbart. För tydlighetens skull indelas behandlingen av personuppgifter närmare i olika delar i paragrafen. Utgångspunkten är att man med behandling av personuppgifter avser alla åtgärder i anslutning till behandlingen av personuppgifter. I detta sammanhang nämns som en särskild tröskel registreringen av personuppgifter. Uppdelningen ger uttryck för att jämförelsen ska leda till att personer för vilka de lagstadgade förutsättningarna inte har uppfyllts inte ska nå militärunderrättelsemyndighetens register.

Paragrafens 2 mom. handlar om att man till en separat del av militärunderrättelsemyndighetens datasystem för de personuppgifter för vilka landets försvar eller den nationella säkerheten har föreskrivits som det ursprungliga eller något annat än det ursprungliga användningsändamålet. Behandlingen av uppgifter sker i sin helhet i ett datasystem med hög informationssäkerhetsnivå utan onödiga överföringar av uppgifterna till datasystem med lägre informationssäkerhetsnivå, vilket väsentligt höjer informationssäkerheten. Förfarandet behövs också med anledning av de informationssäkerhetskrav som beskrivs ovan.

Syftet med bestämmelsen är att göra det möjligt att använda uppgifterna i situationer när behovet av att behandla samma uppgifter är återkommande. Av denna orsak, i motsats till i fråga

om uppgifterna enligt 1 mom., behöver uppgifterna inte raderas omedelbart efter jämförelsen, om man vet att jämförelsen ska göras upprepade gånger. Ett insamlat dataset ska dock förstöras genast när syftet med behandlingen av uppgifterna har uppnåtts. Med datamängd avses i detta sammanhang en icke närmare definierad utifrån sitt användningsändamål avgränsad grupp, som kan vara till exempel ett register, en del av ett register, en databas eller konsoliderade uppgifter. I bestämmelsen definieras inte särskilt de personuppgiftskategorier som får jämföras. Därmed kan också särskilda kategorier av personuppgifter bli aktuella. Förfarandet ska tillämpas endast i sådana situationer när det anses vara nödvändigt att överföra en större datamängd från ett informationssystem för att göra behandling av personuppgifter i ett visst definierat syfte möjlig. De insamlade uppgifterna ska hållas åtskilda från andra uppgifter. I praktiken innebär detta att uppgifterna ska bevaras i en del av informationssystemet i fråga om vilken rätten till tillträde är särskilt begränsad. Dessa uppgifter används för landets försvar och för att skydda den nationella säkerheten, vilket är antingen uppgifternas ursprungliga användningsändamål eller något annat än det ursprungliga användningsändamål som föreskrivits för dem.

8 Ikraftträdande

Det föreslås att lagarna ska träda i kraft så fort som möjligt.

9 Förhållande till andra propositioner

Vid den tidpunkt då propositionen gavs behandlade riksdagen regeringens proposition till riksdagen med förslag till lag om ändring av 10 § i grundlagen (RP 50/2026). Den nu behandlade propositionen har inte någon koppling till den nämnda regeringspropositionen och propositionen kan behandlas i en ordning enligt den gällande grundlagen.

Propositionen har ett samband med regeringens proposition till riksdagen med förslag till ändring av lagstiftningen kring civil underrättelseverksamhet, vilken bereds vid inrikesministeriet. I den proposition som är under beredning görs ändringar som motsvarar vad som föreslås i den nu aktuella regeringspropositionen i lagstiftningen om civil underrättelseverksamhet. Regeringens proposition ska överlämnas för att behandlas av riksdagen under höstsessionsperioden 2026. Regeringspropositionerna förutsätter samordning i riksdagen.

10 Förhållande till grundlagen samt lagstiftningsordning

10.1 Allmänna utgångspunkter

Propositionen innehåller reglering som är relevant med tanke på de grundläggande fri- och rättigheter som föreskrivits i grundlagen då befogenheter som utövas inom militär underrättelseinhämtning innebär intrång i en individs 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 man genom att använda metoderna för underrättelseinhämtning ingriper i någon grundläggande fri- och rättighet, såsom skyddet för privatlivet som föreskrivs i 10 § 1 mom. i grundlagen, är målet i tillämpningen av lagen om militär underrättelseverksamhet dock att skydda och trygga andra grundläggande fri- och rättigheter, såsom rätten till liv och personlig säkerhet enligt 7 § i grundlagen och de grunder för statsordningen vilka föreskrivs i 1 kap. i grundlagen, såsom statens självbestämmanderätt.

Människornas kollektiva säkerhet, liksom även samhällets vitala funktioner och ett organiserat samhällsliv, är så viktiga skyddsintressen att det finns ett vägande samhälleligt behov för underrättelsereglering och en godtagbar grund med tanke på systemet med grundläggande fri- och rättigheter.

Även den nationella säkerheten anses vara en godtagbar grund, som grundlagsutskottet påpekat i sin utlåtandepraxis från den senaste tiden. I sin färskaste utlåtandepraxis har grundlagsutskottet konstaterat att staten ska sträva efter den nationella säkerheten och den allmänna ordningen i alla förhållanden (GrUU 16/2022 rd, stycke 10). Vid intresseavvägningen mellan de grundläggande fri- och rättigheterna ska hänsyn dessutom tas till de intressen som ligger till grund för de föreslagna åtgärderna, i synnerhet om åtgärderna i extrema fall rentav kan återföras på den grundläggande rätten till personlig säkerhet (GrUU 37/2022 rd, stycke 8 och där nämnda GrUU 16/2022 rd, stycke 5, se även GrUU 5/1999 rd, s. 2 samt t.ex. GrUU 36/2020 rd, s. 3, GrUU 15/2018 rd, s. 8).

I den konstitutionella bedömningen av metoder för underrättelseinhämtning är det enligt grundlagsutskottet (GrUU 36/2018 rd) delvis möjligt att förlita sig på utskottets praxis avseende hemliga metoder för inhämtande av information och hemliga tvångsmedel (till exempel GrUU 32/2013 rd, GrUU 67/2010 rd, GrUU 66/2010 rd, GrUU 5/1999 rd). På samma gång ska man dock juridiskt sett göra skillnad mellan de omständigheter som berättigar regleringens avvikande karaktär. Praxis för hemliga metoder för underrättelseinhämtning och hemliga tvångsmedel kan enligt grundlagsutskottets uppfattning således inte tillämpas i oförändrad form och utan förbehåll vid en konstitutionell bedömning av lagstiftningen kring metoderna för inhämtande av information. Metoderna för underrättelseinhämtning ska bedömas enligt metod med hänsyn till grundlagsutskottets praxis i fråga om motsvarande hemliga metoder för underrättelseinhämtning och hemliga tvångsmedel på så sätt att underrättelseverksamhetens särskilda karaktär beaktas på behörigt sätt. Grundlagsutskottet betonar att skyddet för privatlivet och personuppgifter ska sättas i proportion till de andra grundläggande fri- och rättigheterna och andra vägande samhällsintressen (GrUU 14/2018 rd, s. 6 och GrUU 5/1999 rd, s. 2/II).

Lagen om militär underrättelseverksamhet trädde i kraft den 1 juni 2019. Enligt lagen är det möjligt att i militär underrättelseinhämtning inhämta information endast om de objekt som räknats upp på uttömmande sätt i lagen och som föreskrivits på ett så specificerat sätt med beaktande av särdragen i underrättelseverksamheten. Objekten för militär underrättelseinhämtning är oftast stater eller andra offentliga sammanslutningar, som faller utanför skyddet för de grundläggande fri- och rättigheterna (RP 309/1993 rd, GrUU 9/2015 rd och GrUU 4/2018 rd) – de grundläggande fri- och rättigheterna skyddar fysiska personer. Även metoderna för underrättelseinhämtning har reglerats på ett så noggrant avgränsat och exakt sätt som möjligt.

Syftet med de ändringar som föreslås i denna regeringsproposition är att i fråga om vissa metoder för underrättelseinhämtning utfärda bestämmelser om preciseringar med vilka underrättelseinhämtningen, i och med att tekniken utvecklas, kan riktas och riktar sig ännu bättre och ännu effektivare mot det avsedda föremålet. Genom ändringarna beaktas därtill de ändringar som ägt rum i säkerhetsmiljön. Främjande av dessa utgångspunkter kan anses ha positiva konsekvenser för de grundläggande fri- och rättigheterna.

I förslaget fastställer de bestämmelser som innebär en ändring av lagen om militär underrättelseverksamhet befogenheterna för en myndighet så noggrant som möjligt och på så sätt att utövning av befogenheterna är tillåten endast i den omfattning som uppdragen förutsätter.

Befogenheterna enligt den föreslagna lagen att ingripa i medborgarnas grundläggande fri- och rättigheter hör endast till tjänstemän som arbetar under tjänsteansvar och som ansvarar även för åtgärder som på deras begäran vidtas av biträdande personer.

Förslag till bestämmelser som gäller befogenheterna ska granskas som helhet tillsammans med den gällande lagen, i synnerhet visavi de allmänna principer som begränsar militär underrättelseverksamhet. Lagen om militär underrättelseverksamhet innehåller detaljerade bestämmelser om genomskärande principer för verksamheten. Dessa är respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna (5 §), proportionalitetsprincipen (6 §), principen om minsta olägenhet (7 §), principen om ändamålsbundenhet (8 §) och förbudet mot diskriminerande underrättelseverksamhet.

Respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna anses vara den mest omfattande av de principer som ska tillämpas. I den föreskrivs att när en militärunderrättelsemyndighet utövar de grundläggande fri- och rättigheterna, de mänskliga rättigheterna samt befogenheterna, ska den bland de motiverade alternativen välja det alternativ som bäst främjar att dessa rättigheter tillgodoses.

Proportionalitetsprincipen styr åtgärderna inom den militära underrättelseinhämtningen på så sätt att de ska vara försvarbara i förhållande till hur viktiga de uppgifter är som erhålls genom informationsinhämtningen, till hur brådskande underrättelseuppdraget är, till det eftersträlvade målet för den militära underrättelseinhämtningen, till föremålet för den militära underrättelseinhämtningen, till den inskränkning av rättigheter som andra orsakas av att en underrättelseåtgärd används samt till andra omständigheter som påverkar saken. Åtgärden ska även ge tillräckliga faktiska möjligheter att uppnå de godtagbara mål som ställts upp för den militära underrättelseinhämtningen.

Enligt principen om minsta olägenhet får man med militärunderrättelsemyndighetens åtgärder inte ingripa i någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenhet än vad som är nödvändigt för att utföra underrättelseuppdraget. Vid inhämtande av information är det inte tillåtet att ingripa i hemligheten i fråga om förtroliga meddelanden på ett annat än på ett så riktat och begränsat sätt som möjligt.

Utifrån principen om ändamålsbundenheten får befogenheter användas endast för det lagstadgade syftet.

Enligt förbudet mot diskriminerande underrättelseverksamhet får inriktningen av en åtgärd inom den militära underrättelseinhämtningen inte utan godtagbart skäl grunda sig på en persons ålder, kön, ursprung, nationalitet, bosättningsort, språk, religion, övertygelse, åsikt, politiska verksamhet, fackföreningsverksamhet, familjeförhållanden, hälsotillstånd, funktionsnedsättning, sexuella läggning eller någon annan orsak som gäller hans eller hennes person. Det kan anses att principen för egen del garanterar en objektiv inriktning till det föremål som fastställts i lagen om militär underrättelseverksamhet.

Syftet med ovan beskrivna principer kan anses vara omständigheter som begränsar prövningsrätten och förebygger godtycklighet och således främjar individens rättsskydd.

Lagförslagen ska utöver 10 § i grundlagen bedömas med tanke på legalitetsprincipen enligt 8 § i grundlagen, egendomsskyddet enligt 15 §, rättsskyddet enligt 21 § och ansvaret för tjänsteåtgärder enligt 118 § och överföring av en förvaltningsuppgift till någon annan än en myndighet enligt 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).

10.2 Lagen om militär underrättelseverksamhet

10.2.1 De allmänna principer som begränsar militär underrättelse

Lagen om militär underrättelseverksamhet innehåller detaljerade bestämmelser om genomskärande principer för verksamheten. Dessa är respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna (5 §), proportionalitetsprincipen (6 §), principen om minsta olägenhet (7 §), principen om ändamålsbundenhet (8 §) och förbudet mot diskriminerande underrättelseverksamhet.

Respekt för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna anses vara den mest omfattande av de principer som ska tillämpas. I den föreskrivs att när en militärunderrättelsemyndighet utövar de grundläggande fri- och rättigheterna, de mänskliga rättigheterna samt befogenheterna, ska den bland de motiverade alternativen välja det alternativ som bäst främjar att dessa rättigheter tillgodoses.

Proportionalitetsprincipen styr åtgärderna inom den militära underrättelseinhämtningen på så sätt att de ska vara försvarbara i förhållande till hur viktiga de uppgifter är som erhålls genom informationsinhämtningen, till hur brådskande underrättelseuppdraget är, till det eftersträlvade målet för den militära underrättelseinhämtningen, till föremålet för den militära underrättelseinhämtningen, till den inskränkning av rättigheter som andra orsakas av att en underrättelseåtgärd används samt till andra omständigheter som påverkar saken. Åtgärden ska även ge tillräckliga faktiska möjligheter att uppnå de godtagbara mål som ställts upp för den militära underrättelseinhämtningen.

Enligt principen om minsta olägenhet får man med militärunderrättelsemyndighetens åtgärder inte ingripa i någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenhet än vad som är nödvändigt för att utföra underrättelseuppdraget. Vid inhämtande av information är det inte tillåtet att ingripa i hemligheten i fråga om förtroliga meddelanden på ett annat än på ett så riktat och begränsat sätt som möjligt.

Utifrån principen om ändamålsbundenheten får befogenheter användas endast för det lagstadgade syftet.

Enligt förbudet mot diskriminerande underrättelseverksamhet får inriktningen av en åtgärd inom den militära underrättelseinhämtningen inte utan godtagbart skäl grunda sig på en persons ålder, kön, ursprung, nationalitet, bosättningsort, språk, religion, övertygelse, åsikt, politiska verksamhet, fackföreningsverksamhet, familjeförhållanden, hälsotillstånd, funktionsnedsättning, sexuella läggning eller någon annan orsak som gäller hans eller hennes person. Det kan anses att principen för egen del garanterar en objektiv inriktning till det föremål som fastställts i lagen om militär underrättelseverksamhet.

Syftet med ovan beskrivna principer kan anses vara omständigheter som begränsar prövningsrätten och förebygger godtycklighet och således främjar individens rättsskydd.

Inriktningen av militär underrättelseinhämtning och avgränsningsmekanismerna har behandlats tidigare i avsnitt 2.2.1 i de allmänna motiveringarna.

10.2.2 Underrättelseinhämtning som avser datatrafik

10.2.2.1 Allmänt

Grundlagens 10 § innehåller bestämmelser om skyddet för privatlivet. Bestämmelsen tryggar att var och en har rätt till förtrolig kommunikation utan att externa på obehörigt sätt får information om innehållet i förtroliga meddelande som han eller sändaren eller som anvisats till honom eller henne. Detta innebär ett skydd till exempel 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. Dessutom skyddar bestämmelserna i grundlagen även identifieringsuppgifter om avsändaren och mottagaren av ett meddelande och andra uppgifter som kan vara av betydelse för att meddelandet fortsättningsvis är förtroligt.

Enligt 10 § 4 mom. i grundlagen kan genom lag föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång, vid säkerhetskontroll och under frihetsberövande samt för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten. De möjligheter att begränsa skyddet för hemligheten i fråga om förtroliga meddelanden vilka har föreskrivits i bestämmelsen har i samband med revideringen av de grundläggande fri- och rättigheternas avsetts vara en uttömmande förteckning (RP 309/1993 rd, s. 58).

Bestämmelsen skyddar inte innehållet i en diskussion som förs på hörselavstånd och som kan höras med sinnesförmågor, men avlysning med tekniska hjälpmedel av en diskussion som av hävd avsetts vara förtrolig innebär en begränsning av skyddet för hemligheten i fråga om förtroliga meddelanden (RP 309/1993 rd, s. 59, GrUU 11/2005 rd, s. 4, GrUU 36/2002 rd, s. 6, GrUU 2/1996 rd, GrUU 5/1999 rd, s. 4).

Grundlagsutskottet har i sin utlåtandeprocess (GrUU 26/2025 rd, s. 5) i fråga om begränsningarna att tillämpa bestämmelsen betonat att inhämtande av information om verksamhet som hotar den nationella säkerheten utifrån 10 § 4 mom. kan anförtros endast de myndigheter som svarar för den nationella säkerheten, vilka för närvarande är Försvarsmakten och skyddspoliserna.

För det andra gäller begränsningsförutsättningen endast inhämtande av information från sådan verksamhet som är militär eller som på grund av dess natur kan bli ett allvarligt hot mot den nationella säkerheten.

För det tredje ska man genom lag utfärda uttömmande bestämmelser om hur befogenheterna riktas mot militär verksamhet eller verksamhet som allvarligt äventyrar den nationella säkerheten.

För det fjärde möjliggör inte regleringen i 10 § 4 mom. i grundlagen allmän, icke-inriktad och allomfattande uppföljning av datatrafik i underrättelseverksamhet.

Enligt utskottet (GrUU 26/2025 rd, punkt 15) avser nödvändighetskriteriet dels att en begränsning av hemligheten i fråga om förtroliga meddelanden är tillåten bara om det inte är möjligt att inhämta information genom mindre ingrepp, dels att informationsinhämtningen gör intrång på meddelandehemligheten så riktad och begränsad som möjligt. Som princip för den konstitutionella tolkningen betonade utskottet också att grundlagen föranleder ett behov att å

ena sidan tolka begreppet nationell säkerhet restriktivt och å andra sidan ha en hög allvarlighetsgrad i fråga om hot.

Enligt grundlagsutskottet (GrUU 26/2025 rd, punkt 15) har den som åberopar begränsningsgrunden också skyldighet att komma med en tillräcklig motivering till att verksamheten i fråga kan bli ett allvarligt hot mot den nationella säkerheten. För att uppfylla nödvändighetskravet räcker det enligt grundlagsutskottet inte med att inhämtningen av information om förtroliga meddelanden överlag kan anses främja den nationella säkerheten (GrUB 4/2018 rd, s. 8–9).

Bestämmelserna om grundläggande fri- och rättigheter skyddar fysiska personer och juridiska personer indirekt. Staten och andra offentliga sammanslutningar lämnar utanför skyddet för de grundläggande fri- och rättigheterna (RP 309/1993 rd, GrUU 9/2015 rd och GrUU 4/2018). Kommunikationen i en främmande stats myndighetsorganisation åtnjuter inte skydd för hemligheten i fråga om förtroliga meddelanden. För att upptäcka sådan kommunikation är det dock nödvändigt att ingripa i skyddet för förtrolig kommunikation. 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).

I Europadomstolens avgörandepraxis kan djupet på intrång i skyddet för privatlivet genom databehandling med befogenheter som liknar befogenheterna avseende datatrafik delas in i fyra nivåer (Big Brother Watch punkt 325 och Centrum för Rättvisa punkt 239). I det första skedet handlar det om insamling och lagring av datatrafik, i det andra skedet riktas sökbegrepp mot datatrafiken för att filtrera datatrafiken till vad som är väsentligt, i det tredje skedet sätter man sig in i den återstående informationen och i det fjärde och sista skedet används den analyserade informationen och den sprids till dem som behöver den. Europadomstolen anser att insamling av datatrafik inte ännu i sig innebär något djupt ingrepp i skyddet för personens integritet, medan ingreppet är djupast då en myndighet tar del av kommunikationen och utarbetar en rapport utifrån de uppgifter som den fått. Då en tjänsteman från myndigheten sätter sig in i det filtrerade materialet, förutsätter detta på motsvarande sätt den allra kraftigaste övervakningen och andra garantier för rättsskydd. Det ovan nämnda undanröjer dock inte kravet på att bestämmelser ska utfärdas även om myndighetens möjlighet att kunna samla in datatrafik.

Det ska därtill konstateras att grundlagsutskottet uttryckligt konstaterat att meddelandets innehåll inte förlorar det skydd som grundlagen ger enbart om man till exempel har fått information om det genom teleavlyssning (GrUU 99/2022 rd, stycke 12).

Paragraferna 66, 67 a, 68 och 70 § i den nu behandlade propositionen ingriper i skyddet för ett förtroligt meddelande. Bestämmelserna ska bedömas med tanke på 10 § 4 mom. i grundlagen.

10.2.2.2 Behandling av tekniska data

Förhållandet till förmedlingsuppgifter

Enligt 66 § i lagförslag 1 i propositionen får tekniska data behandlas 1) för statistisk analys i syfte att inrikta underrättelseinhämtning som avser datatrafik på en del av kommunikationsnätet, och 2) för övervakning av dirigeringen av och ändringar i datatrafiken. Enligt 10 § 11 punkten

lagen om militär underrättelseverksamhet avses med datatrafikens tekniska data andra uppgifter om datatrafiken än de som hör till innehållet i ett meddelande.

Dessutom skyddar bestämmelserna i 10 § i grundlagen identifieringsuppgifterna om avsändaren och mottagaren av ett meddelande och andra uppgifter som kan vara av betydelse för att meddelandet fortsättningsvis är förtroligt. Förmedlingsuppgifter om kommunikationen omfattas av skyddet för hemligheten i fråga om förtroliga meddelanden enligt 10 § 2 mom. i grundlagen (RP 309/1993 rd, s. 57).

Med tanke på den bedömda regleringen är det relevanta att grundlagsutskottet i sin tidigare praxis ansett att identifieringsuppgifterna för ett förtroligt meddelande har legat utanför kärnområdet för den grundläggande fri- och rättighet som skyddar hemligheten i fråga om förtroliga meddelanden (se till exempel GrUU 33/2013 rd, s. 3, GrUU 6/2012 rd, s. 3–4, GrUU 29/2008 rd, s. 2 och GrUU 3/2008 rd, s. 2). Detta har inneburit att det särskilda lagförbehåll som ingår i nuvarande 10 § 4 mom. i grundlagen inte tillämpats i oförändrad form på begränsning av hemligheten för förmedlingsuppgifter. Reglering som ingriper i skyddet för hemligheten i fråga om förmedlingsuppgifter ska dock enligt utskottets praxis ha uppfyllt de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna (GrUU 62/2010 rd, s. 4/II, GrUU 23/2006 rd, s. 2–3). Således har det till exempel varit möjligt att utfärda bestämmelser om en befogenhet till teleövervakning även i situation där det inte nödvändigtvis handlat om brott som äventyrar individens eller samhällets säkerhet eller hemfriden i enlighet med nuvarande 10 § 4 mom. i grundlagen (GrUU 33/2013 rd, s. 3). Det har ansetts vara möjligt att få identifieringsuppgifter även i vissa situationer som inte handlat om begränsningsgrunder enligt nuvarande 10 § 4 mom. i grundlagen (GrUU 62/2010 rd, s. 4/II).

Därefter har utskottet justerat denna praxis, eftersom identifieringsuppgifter som anknyter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem kan vara så pass problematiska med hänsyn till skyddet för privatlivet att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är (GrUU 18/2014 rd, s. 6/II).

Grundlagsutskottet har i sin utlåtandep Praxis om Gränsbevakningsväsendets radiotekniska övervakning (GrUU 15/2024 rd, punkt 12–13) ansett att det är möjligt att identifiera en radioutrustning, om kommunikationsuppgifterna inte används för att identifiera radioutrustningens ägare eller innehavare. Identifieringen ska i praktiken ske genom tekniska metoder och med den är det möjligt att avgränsa onödiga objekt utanför kretsen för radioteknisk övervakning. Den radiotekniska övervakning som varit föremål för utlåtandet kan hänföra sig till en obegränsad grupp av radioutrustning inom verksamhetsområdet för den tekniska utrustningens sensorer. Grundlagsutskottet ansåg att regleringen ska bedömas via de allmänna förutsättningarna för att begränsa de grundläggande fri- och rättigheterna.

Enligt det nu behandlade förslaget till bestämmelse hänför sig behandlingen av tekniska data till tekniska data som gäller datatrafiken, det vill säga till uppgifter som gäller annat än meddelandets innehåll. Med tanke på grundlagen handlar det i praktiken om förmedlingsuppgifter som gäller kommunikation och olika tekniska data om anordningar som förmedlar elektronisk kommunikation och andra tekniska som jämföras med de sista nämnda. Uppgifterna kan behandlas endast för de syften som angetts noggrant i bestämmelsen, vilka är statistisk analys för att rikta underrättelseinhämtning som avser datatrafik till en del av kommunikationsnätet samt dirigeringen av datatrafiken och bevakning av ändringar. Det handlar om tekniskt riktande i verksamhetsmiljön och teknisk utveckling av systemet för underrättelseinhämtning som avser datatrafik genom att analysera uppgifterna. Tekniska data

som gäller datatrafik behandlas inte för att identifiera objekt för militär underrättelseinhämtning eller personer, utan det handlar om tekniskt riktande i verksamhetsmiljön och teknisk utveckling av systemet för underrättelseinhämtning som avser datatrafik genom att analysera uppgifterna.

Utöver att lagen om militär underrättelseverksamhet innehåller separata bestämmelser om allmänna principer för verksamheten (såsom principen om ändamålsbundenhet), föreslås det att bestämmelsen innehåller uttryckliga bestämmelser om att det i behandlingen av tekniska data inte är möjligt att det uppkommer en analys (genom att slå samman uppgifter), utifrån vilka det är möjligt att direkt identifiera en enskild person. Även om tekniska data kan innehålla också uppgifter som ska ses som personuppgifter, är deras natur av personuppgifter inte av betydelse med tanke på förslaget till bestämmelse i den verksamhet som avses i förslaget till bestämmelse och de får inte heller i övrigt användas för andra syften än de som avgränsats noggrant i bestämmelsen, det vill säga endast som tekniska data. Det finns separata bestämmelser om behandling av personuppgifter i lagen om behandling av personuppgifter inom Försvarsmakten.

Längden på insamlingen av datatrafik i behandlingen av tekniska data

Det föreslås att den gällande paragrafen ändras i 66 § i lagförslag 1 i propositionen på så sätt att man från bestämmelsen stryker den avgränsning som gäller att insamlingen av datatrafik ska pågå kortvarigt.

Grundlagsutskottet ansåg i sitt utlåtande om lagen om militär underrättelseverksamhet (GrUU 36/2018 rd, s. 22–23) att ordalydelsen i 63 § (gällande 66 §) i förslaget till lag om militär underrättelseverksamhet enligt grundlagsutskottets uppfattning verkade möjliggöra insamling och lagring av uppgifter från ett väldigt brett område av ett kommunikationsnät och att det utöver omnämnandet av ”kortvarighet” i 63 § i den föreslagna lagen (gällande 66 §) inte fanns några uttryckliga begränsande kriterier för att samla in och lagra uppgifter. Grundlagsutskottet ansåg att det till denna del var möjligt att i den föreslagna regleringen se särdrag av så kallad massaövervakning, då det även utifrån motiveringarna i propositionen (RP 203/2017 rd, s. 290) var möjligt att kortvarigt behandla tekniska data om datatrafik med inriktning på all datatrafik som rör sig i en del av kommunikationsnätet. Grundlagsutskottet ansåg att bestämmelsen förutsatte att ett förbud mot att på ett allmänt och oriktat sätt bevaka datatrafik ska föreskrivas genom lag, så att bestämmelsen kan kunna behandlas i vanlig lagstiftningsordning.

Grundlagsutskottet har ansett att fjärrstyrning av en obemannad luftfarkost med exempelvis en mobiltelefon eller dator inte handlar som sådan förtrolig kommunikation som avses i 10 § 2 mom. i grundlagen, för vilken man överlag avsett att ge ett grundlagsstadgat skydd via den ifrågavarande bestämmelsen i grundlagen (GrUU 22/2020 rd). Även om man till exempel i kommunikationen mellan en fordonsförare och trafikstyrningen i sig kunde förmedla även förtroliga meddelanden mellan personerna, handlade frågan om undersökning av naturen på exceptionell verksamhet och medvetenheten om lagring av personernas meddelanden enligt utskottet dock inte om verksamhet som omfattas av skyddet för hemligheten i fråga om förtroliga meddelanden enligt 10 § i grundlagen (GrUU 62/2010 rd, s. 5). Även Gränsbevakningsväsendets radiotekniska övervakning ansågs delvis hänföra sig till sådan meddelandetrafik som inte omfattas av skyddet för förtroliga meddelanden enligt 10 § 2 mom. i grundlagen (GrUU 15/2024 rd, stycke 9).

Utskottet har i sin praxis från den senaste tiden ansett att regleringen kring exempelvis Gränsbevakningsväsendets radiotekniska övervakning, i den omfattning som föreslogs vid den tidpunkten, med beaktande av de begränsningar som föreslagits i lagen för övervakningen, var en relativt liten inskränkning av skyddet för hemligheten i fråga om förtroliga meddelande.

Utskottet bedömde även regleringen med tanke på de allmänna förutsättningarna för att begränsa de grundläggande fri- och rättigheterna (GrUU 15/2024 rd, styckena 12–13). Grundlagsutskottet ansåg att det var problemfritt med tanke på grundlagen att behandla förmedlingsuppgifter om radiokommunikation på ett tidsmässigt obegränsat sätt och på så sätt att den hänförde sig till anordningar som inte specificerats i ett visst geografiskt område eller i dess omedelbara närhet. Utplåning av uppgifter, behandling av personuppgifter och utplåning av personuppgifter föreskrivs separat i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet. Beslutet om radioteknisk övervakning fattas av chefen för gräns- och sjöbevakningsavdelningen vid Gränsbevakningsväsendets stab.

Det nu behandlade förslaget till bestämmelse hänför sig till uppgifter som utgör tekniska data som producerats av olika tekniska styrnings- och andra anordningar i ett datatrafiksnätet, men även förmedlingsuppgifter. I fråga om styrnings- och andra anordningar kan förslaget till bestämmelse anses vara problemfritt med tanke på grundlagen.

I fråga om förmedlingsuppgifter, även om det handlar om personuppgifter, får de enligt förslaget till bestämmelse inte behandlas på ett sätt som gör att en enskild fysisk person kan identifieras utifrån dessa. Således är det inte utifrån endast en förmedlingsuppgift möjligt att dra slutsatser om en enskild persons verksamhet, såvida inte informationen slås samman med annan information och man på så sätt utreder den som använt förmedlingsinformationen och hans eller hennes privatliv. Förslaget till bestämmelse ger inte möjlighet till detta. Dessutom styrs verksamheten av till exempel principen om ändamålsbundenhet.

Det kan inte anses att förslaget till bestämmelse handlar om allmän och oinriktad underrättelseinhämtning som avser datatrafik, eftersom det handlar om maximalt noggrann inriktning av den egentliga underrättelseinhämtningen som avser datatrafik. Förslaget till bestämmelse kan inte heller anses utgöra allmän underrättelseinhämtning som avser datatrafik, eftersom befogenheten hänför sig till en viss del av ett kommunikationsnät som överskrider Finlands gräns och tekniska data om den datatrafik som rör sig i den under en viss tidpunkt. Genom befogenheten genomförs inte heller något underrättelseuppdrag, utan det handlar om inhämtning av den information som underrättelseuppdraget förutsätter i fråga om datatrafikens och det gränsöverskridande datakommunikationsnätets tekniska egenskaper. Till andra delar än i fråga om tekniska data om datatrafik ska uppgifterna utplånas även utifrån regleringen om utplåning.

Beslutet om verksamheten enligt förslaget till bestämmelse fattas av en domstol och tillståndets giltighet är avgränsad till sex månader. Giltighetstiden motsvarar vad som föreskrivs i fråga om egentlig underrättelseinhämtning som avser datatrafik i den gällande lagen. Behandlingen av tekniska data hänför sig till tekniska data om datatrafiken och utifrån dessa är det inte möjligt att direkt identifiera en enskild person eller på ett avsevärt sätt ingripa i skyddet för privatlivet för en person. Den föreslagna bestämmelsen innehåller vidare ett förbud att i behandlingen av tekniska data bilda en analys utifrån vilken en enskild person kan identifieras. Förbudet kan anses betona principen om ändamålsbundenhet, som föreskrivs i grundlagen och lagen om militär underrättelseverksamhet.

Förslaget till bestämmelse ingriper i det integritetsskydd som tryggas i 10 § i grundlagen, men med stöd av bestämmelsen behandlas tekniska data som gäller datatrafik ur en teknisk synvinkel. Utifrån det ovan konstaterade kan förslaget till bestämmelse behandlas i lagstiftningsordningen för en vanlig lag med stöd av 10 § 4 mom. i grundlagen. Bättre analys av tekniska data som gäller datatrafiken kan anses ha positiva konsekvenser för de grundläggande fri- och rättigheterna, eftersom den kan bedömas förbättra inriktningen av den egentliga informationsinhämtningen som avser datatrafik.

10.2.2.3 Fastställande av sökbegrepp

Fastställande

Genom 67 a § i lagförslag 1 i propositionen görs ett intrång i meddelandets innehåll. Enligt 1 mom. i paragrafen får Försvarsmaktens underrättelsetjänst samla in och lagra datatrafik i en del av ett kommunikationsnät som överskrider Finlands gräns i syfte att noggrannare inrikta underrättelseinhämtning som avser datatrafik och behandla den, om det är nödvändigt för att fastställa nya sökbegrepp som beskriver föremålet. Den datatrafikmängd som inhämtas och lagras får inte överskrida fem procent av kapaciteten i en del av ett kommunikationsnät som överskrider Finlands gräns. Sökbegrepp har enligt 10 § 1 punkten i lagen definierats som en uppgift som används för att vid underrättelseinhämtning som avser datatrafik så avgränsat och exakt som möjligt i en del av kommunikationsnätet selektera den datatrafik som är föremål för underrättelseinhämtningen, varvid intrånget i skyddet för hemligheten för förtroliga meddelanden sker endast i den omfattning som är nödvändig för att uppnå syftet med underrättelseinhämtningen. Definitionen har utarbetats med riksdagens medverkan (FöUB 9/2018 rd, GrUU 36/2018 rd och GrUU 76/2018 rd). Eftersom sökbegreppet avgränsar den information som fås genom underrättelseinhämtning som avser datatrafik endast till vad som är nödvändigt med tanke på syftet med underrättelseinhämtningen, är det enligt den gällande regleringen inte heller ofta möjligt att fastställa nya sökbegrepp som hänför sig till föremålet för militär underrättelseinhämtning.

I sin praxis har grundlagsutskottet i fråga om teknisk övervakning av radioutrustning ansett att reglering utifrån vilken identifieringen av en anordning som använder elektromagnetiska vågor i praktiken sker med automatiska tekniska metoder och man genom den avgränsar obehövliga objekt från den radiotekniska övervakningen är problemfri med tanke på de grundläggande fri- och rättigheterna (GrUU 15/2024 rd, punkt 12). Enligt motiveringarna till bestämmelsen har den information som tagits fram genom radioteknisk övervakning filtrerats till sådan form att slutanvändaren inte får kännedom om de identifieringsuppgifter som används för att identifiera en radioutrustning.

Fastställandet av nya sökbegrepp hänför sig till datatrafikflödet i dess maskinspråkform, utifrån vilken det före den tekniska behandlingen av datatrafiken inte är möjligt att direkt utreda och läsa förmedlingsuppgifter eller innehållet i ett meddelande – datatrafikflödet handlar om teckensträngar, i binärform (serier som bildas av siffrorna 1 och 0) utifrån vilken exaktare uppgifter inte kan avläsas. Vilken ordning tecknen antar beror bland annat det datasystem som används av den organisation som sänder det elektroniska meddelandet, de andra använda anordningarna samt programvarorna. Dessutom påverkar bland annat de använda protokollen teckensträngarna.

Enligt det nu behandlade förslaget till bestämmelse behandlas datatrafikflödet med automatiska och manuella tekniska metoder för att fastställa sökbegrepp. I fastställandet är det förbjudet att använda uppgifter i meddelandet betydelseinnehåll. I fastställandet av sökbegrepp får man inte heller kombinera uppgifter på ett sätt som gör att meddelandets semantisk innehåll klarnar och inte heller information utifrån vilken det är möjligt att dra slutsatser om någon persons privatliv. Syftet med den föreslagna befogenheten är inte heller att få uppgifter om en person eller hans eller hennes privatliv, utan syftet är att fastställa sökbegrepp för att rikta underrättelseinhämtning som avser datatrafik till vad som är nödvändigt i enlighet med definitionen av sökbegrepp i lagen.

För att underrättelseinhämtning som avser datatrafik ska vara så riktad som möjligt och för att den ska ge den förväntade begränsade informationen, ska underrättelsemyndigheten ha

förhandsinformation om hur sökbegreppet ska riktas så att den gör intrång i skyddet för kommunikation på ett så avgränsat sätt som möjligt. I det nu behandlade förslaget till bestämmelse baserar sig fastställandet av sökbegrepp på den förmodade regelbundenheten eller särdraget i objektets datatrafik.

Den föreslagna bestämmelsen gäller behandling av datatrafik i dess teknisk form och undersökning och tolkning av teckensträngar i datatrafiken. Myndigheten har en utgångsuppgift om datatrafikens förmodade regelbundenhet eller tekniska särdrag, utifrån vilken sökbegrepp fastställs för datatrafiken. Utifrån de nya sökbegreppen är det möjligt att rikta den egentliga underrättelseinhämtningen som avser datatrafik noggrant mot föremålet för den militära underrättelseinhämtningen. Detta kan anses ha positiva konsekvenser för de grundläggande fri- och rättigheterna, eftersom information som är onödig för den militära underrättelseinhämtningen kan filtreras bort direkt redan i initialskedet.

Eftersom målet för befogenheten utgörs av datatrafikflödet, kan de uppgifter som utgör föremål för användning av befogenheten anses vara anonymiserade i den mån att det utifrån dessa inte är möjligt att direkt utreda uppgifter om en enskild persons privatliv eller innehållet i kommunikationen på ett sätt som avsevärt ingriper i skyddet för privatlivet eller hemligheten i fråga om ett meddelande. För att uppgifterna ska kunna utredas, förutsätter detta enligt lagförslaget användning av en egentlig metod för underrättelseinhämtning (68 och 70 §). I annat fall görs en överträdelse av de allmänna principerna i lagen om militär underrättelseverksamhet och även i övrigt gör sig myndigheten skyldig till brottslig verksamhet.

Användningen av befogenheten är bunden till nödvändighet. I detta fall innebär nödvändighet att nya sökbegrepp i praktiken inte kan fastställas på ett annat sätt eller så kräver fastställandet orimliga resurser.

Så som redan konstaterats har grundlagsutskottet i sin utlåtandepraxis konstaterat att underrättelseinhämtning som avser datatrafik inte kan vara allmän, oinriktad och allmäntäckande bevakning av datatrafik (GrUU 36/2018 och GrUB 4/2018 rd, s. 8). Denna begränsning har beaktats i 65 § i lagen om militär underrättelseverksamhet. Å andra sidan har Europadomstolen i sin nyaste avgörandepraxis ansett att insamling av datatrafik, även om den hänför sig till en stor grupp personer, inte i sig ingriper i skyddet för personens integritet på ett lika omfattande sätt som i en situation där en analytiker utreder meddelandets innehåll och slår samman uppgifter för att närmare utreda den verksamhet som utgör objekt (bland annat Centrum för Rättvisa, punkterna 239–245).

Fastställande av sökbegrepp enligt det nu behandlade förslaget till bestämmelse kan inte anses vara helt oinriktat, eftersom det baserar sig på den förmodade regelbundenheten eller det förmodade särdraget i objektets datatrafik, vilka ska nämnas i domstolstillståndet. Dessutom ska den förmodade regelbundenheten eller det förmodade särdraget motiveras, det vill säga att det inte är möjligt att fastställa nya sökbegrepp utifrån förhandsinformationen. I enlighet med regleringen om beslutsfattande ska militärunderrättelsemyndigheten således ha en riktgivande uppfattning om datatrafiken hos den aktör som utgör objekt, så att man vid fastställandet av sökbegrepp inte behöver gå igenom all potentiell datatrafik.

Förslaget till bestämmelse kan inte heller anses vara allmänt. Den nu behandlade befogenheten är fysiskt avgränsad till en viss del av ett kommunikationsnät som överskrider Finlands gräns, och därtill har de behandlande mängden uppgifter begränsats till fem procent av kapaciteten i denna del av kommunikationsnätet, det vill säga till den mängd som en delen av kommunikationsnätet tekniskt sett maximalt kan transportera.

På ovan beskrivna sätt kan det inte anses att de uppgifter som skaffas genom den föreslagna befogenheten innebär något djupt ingrepp i skyddet för ett privat meddelande. En djup inskränkning förutsätter att de uppgifter som innehas av militärunderrättelsemyndigheten slås samman med den datatrafik som utgör objekt samt att andra metoder för underrättelseinhämtning används.

Den föreslagna bestämmelsen innehåller ett förbud enligt vilket information som beskriver en enskild person eller innehållet i meddelandet inte får uppkomma i analysen. Behandlingen av datatrafiken sker i den tekniska formen för datatrafiken, det vill säga på maskinspråk.

I 67 b § i lagförslag 1 i propositionen utfärdas bestämmelser om beslutsfattande om befogenheten enligt 67 a §. I ett yrkande och ett beslut ska man redogöra för underrättelseuppdraget och fakta som gäller det. I ett yrkande ska man därtill motivera nödvändigheten.

Som en central omständighet ska man i ett yrkande och ett beslut föra fram de förmodade regelbundenheterna eller särdragen i objektets datatrafik, på basis av vilka sökbegreppen fastställs, samt motiveringarna till dem. I enlighet med punkten ska militärunderrättelsemyndigheten ha en riktgivande uppfattning om datatrafiken hos den aktör som utgör objekt, så att man vid fastställandet av sökbegrepp inte behöver gå igenom all potentiell datatrafik. I ett yrkande ska man även motivera varför nya sökbegrepp kan fastställas utifrån denna förhandsinformation. Även underrättelseuppdraget ska nämnas i tillståndet.

Även om befogenheten i sig tydligt innebär ett ingrepp i kommunikationens innehåll, kan ingreppsgraden inte anses motsvara vad som 68 och 70 § i lagen handlar om. Fastställandet av närmare sökbegrepp, vilket är målet med den föreslagna bestämmelsen, kan anses ha positiva konsekvenser för de grundläggande fri- och rättigheterna.

Utifrån ovan beskrivna grunder kan förslaget till bestämmelse inte anses ingripa i skyddet för hemligheten i fråga om ett privat meddelande på ett sätt som är lika betydande som vid egentlig informationsinhämtning som avser datatrafik (68 och 70 § i lagen). Således kan bestämmelsen behandlas i vanlig lagstiftningsordning i enlighet med 10 § 4 mom. i grundlagen.

Giltighetstiden för ett tillstånd

Enligt 67 b § i lagförslag 1 kan ett tillstånd för att fastställa sökbegrepp beviljas för sex månader åt gången. Tidsperioden motsvarar vad som föreslås om giltighetstid för ett tillstånd för behandling av tekniska data och å andra sidan den giltighetstid som redan i den nuvarande lagen finns för ett tillstånd till informationsinhämtning som avser datatrafik.

Grundlagsutskottet har riktat uppmärksamhet på giltighetstiderna för tillstånd (GrUU 35/2018 rd och GrUU 36/2018 rd) genom att hänvisa till utvecklingen i Europadomstolens avgörandepraxis. Grundlagsutskottet har hänvisat till fallen Centrum för Rättvisa och Big Brother Watch. I bägge fall konstaterades att informationsinhämtningen var möjligt enligt Europakonventionen, om den baserade sig på ett domstolstillstånd och längden av informationsinhämtningen var högst sex månader. Europadomstolen betonade vikten av att det finns självständiga organ som övervakar underrättelseverksamhet för systemets godtagbarhet.

I det fall som nu behandlas övervakas verksamheten av flera självständiga organ. Dessutom bedöms intrånget i skyddet för en privatpersons kommunikation på grund av verksamhet enligt föreslagna 67 a § inte vara lika djupt som egentlig underrättelseinhämtning som avser datatrafik

enligt 68 och 70 § i lagen. Giltighetstiden på sex månader för ett tillstånd kan anses vara problemfri med tanke på grundlagen.

10.2.2.4 Lagringstiden för tekniska data och datatrafik

Lagringstiden

I 66 § 2 mom. och 67 a § 4 mom. i lagförslag 1 i propositionen finns det bestämmelser om särskilda lagringstider. I fråga om tekniska data är lagringstiden 18 månader och i fråga om uppgifter som används för att fastställa sökbegrepp är lagringstiden tolv månader.

Grundlagsutskottet har tagit ställning (GrUU 18/2014 rd) till lagringstiderna för uppgifter i en situation där teleföretagen åläggs att lagra alla uppgifter om deras abonnenter under den tid som föreskrivits närmare i lagen. Regeringens proposition, som utlåtandet var föremål för, gällde upphävandet av det så kallade Data Retention-direktivet. Grundlagsutskottet har ansett att en tid på tolv månader från den dag då kommunikationen ägde rum är godtagbar med tanke på proportionaliteten och motsvarar myndigheternas behov (GrUU 3/2008 rd). Grundlagsutskottet (GrUU 15/2024 rd) har även ansett i fråga om Gränsbevakningsväsendets radiotekniska övervakning att det är godtagbart att upptagningar som uppkommit i övervakningen och som ännu är oriktade kan förvaras i ett år efter upptagningen uppkommit. För att rikta den radiotekniska övervakningen och avskilja och avgränsa övervakningsobjekten raderas de personuppgifter som behandlas senast fem år efter att de införts i registret.

Grundlagsutskottet har i sin utlåtandepraxis ansett att det inte är något problem att personuppgifter lagras i över ett år (GrUU 21/2013 rd och GrUU 13/2017 rd), även om personen inte misstänks ha någon koppling till verksamhet som till exempel allvarligt hotar den nationella säkerheten. Utskottet har riktat uppmärksamhet på att ju längre tid uppgifter lagras, desto väsentligare är det att säkerställa dataskyddet, övervakningen av användningen av uppgifterna och de registrerades rättsskydd (bland annat (GrUU 28/2016 rd).

I fråga om teleföretagens allmänna och ospecificerade skyldighet att lagra identifieringsuppgifter har grundlagsutskottet konstaterat (GrUU 35/2004 rd) att lagringen av identifieringsuppgifter enligt utskottets mening alltid är förknippad med risker, såväl i fråga om skyddet för förtroliga meddelande som i fråga om skyddet för personuppgifter. Riskerna ökar, ju längre uppgifterna lagras. Till exempel har en lagringstid på tre år ansetts vara exceptionellt lång med tanke på den allmänna personuppgiftslagstiftningen (GrUU 35/2004 rd, s. 4 och GrUU 26/1998 rd, s. 3).

Det väsentliga med tanke på de nu behandlade förslagen är vilka uppgifter som lagras, hur omfattande lagringen av uppgifter är, hur lång lagringstiden är och för vad lagrade uppgifter får användas. Dessutom är det av betydelse i vilken form uppgifterna är.

I fråga om tekniska data handlar det om behandling av tekniska data om datatrafik. I behandlingen av tekniska data behandlas tekniska data om datatrafik för att identifiera en del av ett visst kommunikationsnät och för att följa dirigeringen av och ändringar i datatrafiken. Det handlar om en teknisk analys och uppgifterna innehåller inte något meddelandeinnehåll. Utifrån tekniska data, även om de är personuppgifter, är det inte möjligt att göra djupgående slutsatser om en persons privatliv.

I 66 § 3 mom. i lagförslag 1 är lagringstiden 18 månader från det att tekniska data om datatrafik har samlats in. Den lagrade mängden tekniska data får vara fem procent av kapaciteten i den del av ett kommunikationsnät som överskrider Finlands gräns, det vill säga av den maximala mängd

datatrafik som en del av ett kommunikationsnät tekniskt sett kan transportera. Tekniska data som gäller datatrafiken innehåller även förmedlingsuppgifter, men i oförändrad form är det inte möjligt att utifrån dessa identifiera en person som använder förmedlingsuppgifter eller i övrigt ingripa i hans eller hennes rättigheter på avsevärt sätt. Andra tillståndspliktiga åtgärder förutsätts för att identifiera en person. Innehåll i kommunikationen filtreras inte till lagringen. Efter lagringstidens utgång raderas de lagrade uppgifterna automatiskt.

Den föreslagna lagringstiden på 18 månader kan anses vara nödvändig för att historikdata även ska vara i användning i behandlingen av tekniska data. Historikdata är av väsentlig relevans i identifieringen av en del av kommunikationsnät så att det exempelvis ska vara möjligt att identifiera regelbundenheter i datatrafik som kommer från ett visst område. Dessutom är historikdata nödvändiga för att identifiera anordningar och topologier som används i ett globalt datatrafiksnät. Med den nuvarande takten på den tekniska utvecklingen kan 18 månader ses som en tidsperiod under vilken det är möjligt att upptäcka de mest betydelsefulla tekniska ändringarna i ett datatrafiksnät. Under denna tidsperiod hinner militärunderrättelsemyndigheten även reagera på tekniska förändringar i ett globalt kommunikationsnät. Uppgifterna är även av betydelse för det föreslagna fastställandet av sökbegrepp enligt 67 a § och i egentlig underrättelseinhämtning som avser datatrafik (68 och 70 §).

Vid verksamhet enligt det behandlade förslaget till bestämmelse får man inte inhämta information om underrättelseobjekten, utan det handlar om teknisk bevakning av datatrafiken. Således kan lagringstiden på 18 månader inte anses vara problematisk med tanke på grundlagen.

Enligt 67 a § 4 mom. i nu behandlade lagförslag 1 är lagringstiden tolv månader. Den föreslagna tidsperioden är kortare än vad som föreskrivs i föreslagna 66 §. Fastställandet av sökbegrepp enligt den föreslagna bestämmelsen sker i ett skede där det utifrån datatrafiken inte är möjligt att direkt utreda meddelandets semantiska innehåll. Lagringen av datatrafik sker i den teknisk formen för datatrafiken (bit och byte), varför utredning av det semantiska innehållet i sparad datatrafik och utredning av om datatrafiken innehåller information som hänför sig till objektet för den militära underrättelseinhämtningen förutsätter andra tillståndspliktiga åtgärder av militärunderrättelsemyndigheten.

Utöver tekniska data om datatrafiken lagras även en annan del av kommunikationen – lagringstiden ska vara kortare än för tekniska data. Lagringen kan hänföra sig till fem procent av kapaciteten i den del av det kommunikationsnät som utgör föremål för underrättelseinhämtningen, det vill säga till den mängd datatrafik som tekniskt sett högst kan röra sig på en gång i kommunikationsnätets del. Kapaciteten kan utredas bland annat från de tekniska uppgifterna om datatrafikkablarna och -fibrerna. Efter den föreslagna lagringstiden raderas uppgifterna automatiskt från informationssystemet.

Lagring av uppgifter är nödvändig med tanke på fastställandet av sökbegrepp enligt föreslagna 67 a § och den egentliga underrättelseinhämtningen som avser datatrafik (68 och 70 §) för att underrättelseinhämtningen avseende datatrafik ska hänföra sig endast till en nödvändig del av datatrafiken. Jämförelsen av historikdata om datatrafik är en avsevärd del vid fastställande av nya sökbegrepp och vid inhämtande av information om underrättelseobjektet.

De lagrade uppgifterna kan anses kunna utnyttjas i tolv månader, då de lagrade uppgifterna kan anses vara till nytta. I och med att den tekniska utvecklingen är intensiv, finns det inte grunder för en längre lagringstid än den nämnda tidsperioden och uppgifter från en tid före den föreslagna tidsperioden kan anses förlora sin betydelse i förhållande till syftena med förslaget till bestämmelse.

Med tanke på skyddet för integriteten är det även väsentligt att elektroniska meddelanden inte rör sig som en koherent helhet i kommunikationsnätet, utan som datatrafikpaket, som vart och ett rör sig längs den effektivaste ruten till sin destination.

Grundlagsutskottet har ansett att en tolv månader lång lagringstid för uppgifter inte är problematisk i fråga om personuppgifter, även om den på ospecificerat sätt hänför sig till en viss grupp av personer (personer som överskrider Finlands gräns). I den nu behandlade situationen är de uppgifter som ska lagras i den tekniska formen i datatrafiken i systemet, vilken inte direkt kan kombineras med en enskild fysisk person, och utifrån den är det inte heller möjligt att utreda innehållet i ett meddelande. Med stöd av befogenheten är det inte möjligt att skaffa information till exempel om en enskild persons verksamhet.

I enlighet med grundlagsutskottets praxis (bland annat GrUU 28/2016 rd) ombesörjs dataskyddet, övervakningen av användningen av uppgifter och den registrerades rättsskydd vid verksamhet enligt de föreslagna bestämmelserna. Utöver den interna övervakningen sköter underrättelsetillsynsombudsmannen och dataskyddsombudsmannen till centrala delar övervakningen. I fråga om rättsskyddet sköts övervakningen inom ramen för domstolarnas förhandskontroll och därtill av underrättelsetillsynsmyndigheten och dataombudsmannen.

De insamlade och lagrade uppgifterna omfattas även av den lagstadgade allmänna skyldigheten att utplåna uppgifter. Således ska datatrafik utplånas i takt med att den konstateras vara onödig. I varje fall utplånas datatrafiken efter att den föreskrivna utsatta tiden uppnåtts.

Även om förmedlingsuppgifter och datatrafik lagras på ett oriktat sätt i systemet, kan militärunderrättelsemyndigheten inte använda uppgifterna utan ett tillstånd till befogenheten av en domstol, utifrån vilket lagrade uppgifter får användas. Således kan en militärunderrättelsemyndighet inte utreda till exempel användaren av en okänd IP-adress genom att använda 104 § i lagen om militär underrättelseverksamhet om inte informationen fåtts i egentlig underrättelseinhämtning som avser datatrafik (68 eller 70 § i lagen).

Utifrån ovan konstaterade grunder kan de föreslagna lagringstiderna anses vara nödvändiga och förslagen till bestämmelser kan inte anses vara motstridiga med skyddet för hemligheten i fråga om förtroliga meddelanden enligt 10 § i grundlagen.

Användning av lagrade uppgifter

Det föreslås att 66 §, 67 a §, 68 § och 70 § i lagförslag 1 i propositionen innehåller bestämmelser om användning av de lagrade uppgifter som avses i 66 och 67 §. Användningen av uppgifter är graderad enligt hur djupt det är möjligt att göra intrång i skyddet för privatlivet genom befogenheterna. Med andra ord är det möjligt att i behandling av tekniska data (föreslagna 66 §) använda endast tekniska data, i fastställandet av sökbegrepp (föreslagna 67 a §) är det möjligt att använda tekniska data och fem procent av datatrafik i den del av kommunikationsnätet som utgör objekt och i egentlig underrättelseinhämtning som avser datatrafik (68 och 70 §), som innebär det djupaste intrången i skyddet för privatlivet, är det möjligt att använda lagrade tekniska data och uppgifter som lagrats utifrån fastställandet av sökbegrepp.

En förutsättning för att kunna använda lagrade uppgifter är alltid ett domstolstillstånd i samband med det egentliga tillståndsbeslut om användning av befogenheten.

Med stöd av ovan beskrivna förslag till bestämmelser kan användningen av lagrad information anses delvis ligga nära användningen av överskottsinformation. Med överskottsinformation i brottsbekämpningen avses av hävd information som fåtts genom teleavlyssning,

teleövervakning, inhämtande av basstationsuppgifter och teknisk observation och som inte gäller ett visst brott eller avvärjande av en fara eller som gäller ett annat brott än det för vilket ett tillstånd eller beslut getts i syfte att förhindra eller avslöja det.

Regleringen kring överskottsinformation i polislagen har föreskrivits med grundlagsutskottets medverkan (GrUU 67/2010 rd, s. 4–5, GrUU 33/2013 rd, s. 5–7). Utskottet har granskat regleringen med tanke på hemligheten i fråga om förtroliga meddelanden, vilken tryggats i 10 § i grundlagen. Enligt utskottet står det klar att överskottsinformation som fåtts med ett hemligt tvångsmedel som i sig är lagligt inte kan användas på obegränsat sätt för att utreda vilket brott som helst. Det främsta syftet med den bestämmelse som skyddar hemligheten i fråga om förtroliga meddelanden är att skydda innehållet i konfidentiella meddelanden för utomstående. Meddelandets innehåll går inte miste om det skydd som grundlagen ger enbart utifrån att man till exempel har fått information om det genom teleavlyssning. Regleringen i 10 § i grundlagen begränsar användningen av innehållet i ett meddelande även efter detta. Detta är väsentligt även därför att även en extern person, utöver det egentliga objektet för avlyssningen, kan bli föremål för ett hemligt tvångsmedel. Enligt utskottet ska man därtill observera att om användning av överskottsinformation tillåts för utredning av andra ringare brott än sådana brott som motiverar respektive teletvångsmedel, så innebär detta indirekt en uppluckring av begränsningarna för användning av teletvångsmedel (GrUU 33/2013 rd, s. 6/II). (GrUU 99/2022 rd).

Enligt grundlagsutskottet fanns det inte något hinder för att man i bestämmelsen om användning av överskottsinformation inkluderar vissa sådana enskilda brott vars maximistraff är fängelse i två år, men som dock i fråga om allvarlighetsgrad jämföras med övriga brott som uppfyller förutsättningen för användning av överskottsinformation och som uppfyller de krav som ställs på begränsning av hemligheten i fråga om förtroliga meddelanden i 10 § i grundlagen (GrUU 33/2013 rd, s. 7/I).

Grundlagsutskottet har i fråga om brottsbekämpning förutsatt ett tillstånd som getts av en domstol som en förutsättning för att använda överskottsinformation som fåtts med ett teletvångsmedel (GrUU 66/2010 rd s. 10/II; GrUU 67/2010 rd, s. 5/I).

Den föreslagna rätten enligt 66 §, 67 a §, 68 § och 70 § i lagförslag 1 i propositionen för militärunderrättelsemyndigheten att lagra tekniska data om datatrafiken och sporadisk datatrafik i en del av ett kommunikationsnät som överskrider Finlands gräns kan i fråga om grundläggande utgångspunkter anses vara en situation som motsvarar användning av överskottsinformation inom brottsbekämpning. ”Överskottsinformation” inhämtas i samband med användning av en annan befogenhet (66 § och 67 a §) än den med vilken informationen används (67 a §, 68 och 70 §). Genom de föreslagna ändringarna kan en militärunderrättelsemyndighet lagra information som inte omfattas av det aktuella domstolstillståndet i situationen.

Med undantag för behandling av tekniska data utgörs grunden för tillståndet alltid av militär verksamhet eller verksamhet som allvarligt hotar den nationella säkerheten. I 4 § i lagen om militär underrättelseverksamhet uppräknas på uttömmande sätt verksamhet som kan ligga till grund för användning av underrättelsemetoder. I motsats till brottsbekämpning kan det anses att den verksamhet som ligger till grund för tillståndet inte handlar om lindrigare och allvarligare verksamhet, mot vilken det är möjligt att rikta olika metoder för underrättelseinhämtning, utan all verksamhet som nämns i 4 § är lika allvarlig med tanke på de rättsobjekt som ska skyddas.

Användningen av lagrade uppgifter förutsätter domstolstillstånd, i vilket man i fråga om behandling av andra än tekniska data ska nämna objektet för användningen av metoden för underrättelseinhämtning. Dessutom ska man nämna de omständigheter som är väsentliga för att rikta metoden, såsom regelbundenheten i datatrafiken med tanke på fastställandet av sökbegrepp

eller sökbegreppen i den egentliga underrättelseinhämtningen som avser datatrafik. I fråga om tekniska data har de uppgifter som behandlats även i övrigt avgränsats till tekniska data.

I 67 a § i lagförslag 1 i propositionen utgörs förutsättningen för fastställande av sökbegrepp av nödvändighet, vilket motsvarar vad som redan föreskrivs i den gällande lagen om egentlig underrättelseinhämtning som avser datatrafik. Lagrade uppgifter får inte heller användas för användning av andra metoder än metoder för underrättelseinhämtning enligt föreslagna 66 § och 67 a § och redan föreskrivna 68 § och 70 §.

Genom historikdata beträffande tekniska data är det möjligt att i den egentliga underrättelseinhämtning som avser datatrafik verifiera till exempel om objektet redan tidigare kommunicerat via en del av ett kommunikationsnät som överskrider Finlands gräns. Uppgifterna kan vara nödvändiga till exempel för att säkerställa ett längre umgänge mellan två kommunicerande aktörer (innehållet i meddelandet är inte av betydelse) eller för att säkerställa att så noggranna sökbegrepp som möjligt fastställs.

Förutsättningen för användning av alla ovan nämnda befogenheter är ett domstolstillstånd. En domstol kan även avgränsa användningen av befogenheter så att den helt riktar sig till lagrade uppgifter eller till exempel avgränsa den tidsmässigt. I det yrkande som görs till en domstol ska man även lägga att befogenheten kommer utövas för lagrade uppgifter och motivera detta.

Utifrån ovan avsedda bestämmelser kan lagrade uppgifter inte användas i samband med andra metoder för underrättelseinhämtning än i samband med den helhet som utgörs av underrättelseinhämtning som avser datatrafik.

Det är möjligt att anse att förslaget till bestämmelse förbättrar inriktningen av den helhet som utgörs av informationsinhämtning som avser datatrafik och således kan förslaget till bestämmelse anses ha positiva konsekvenser för de grundläggande fri- och rättigheterna.

10.2.2.5 Informationsinhämtning om datatrafik som gäller föremålet för militär underrättelseinhämtning

Sökbegrepp som hänför sig till innehållet i ett meddelande

Ändringarna av 70 § i lagförslaget ingriper i skyddet för innehållet i en meddelande. Från förslaget till bestämmelse stryks det ovillkorliga förbudet att använda språkliga sökbegrepp som avser innehållet i meddelandet. Det är möjligt att använda språkliga sökbegrepp som gäller innehållet i ett meddelande tillsammans med andra sökbegrepp som beskriver det språkliga innehållet i ett meddelande. Andra än språkliga sökbegrepp som gäller meddelandets innehåll kan finnas även i meddelandets innehåll.

Grundlagsutskottet har inte tagit direkt ställning till förbudet att använda sökbegrepp som gäller innehållet i ett meddelande, med undantag för information som beskriver ett sabotageprogram. I regeringens proposition om 10 § i grundlagen (RP 198/2017 rd) har det konstaterats att kommunikationen av en främmande stats myndighetsorganisation inte åtnjuter skyddet för hemligheten i fråga om förtroliga meddelanden. I sitt betänkande om ändringen (GrUB 4/2018 rd) konstaterade grundlagsutskottet att även om en främmande stats militär- eller en annan myndighetsorganisations kommunikation inte åtnjuter skyddet för hemligheten i fråga om förtroliga meddelanden, kan befogenheter till militärunderrättelseinhämtning i samtliga fall inte riktas så exakt att det inte finns någon fara för att myndigheterna tillfälligt får tillgång till uppgifter om kommunikationen för enskilda personer utan koppling till underrättelseuppdraget, vilket enligt grundlagsutskottets mening ska avgränsas till en så liten omfattning som möjligt i

vanliga lagar. Således har det varit möjligt att använda sökbegrepp som hänför sig till innehållet i ett meddelande i underrättelseinhämtning som hänför sig till en statlig aktörs datatrafik.

I sin nyaste praxis har grundlagsutskottet på ett noggrannare sätt än tidigare bedömt förhållandet mellan ett sabotageprogram och ett kommando och grundlagens 10 § 2 mom. I sitt utlåtande (GrUU 62/2024 rd, punkt 12) om regeringens proposition om en cybersäkerhetslag (RP 57/2024 rd) riktade grundlagsutskottet uppmärksamhet på att sådana i lagförslagen avsedda meddelanden som innehåller ett skadligt datorprogram eller kommando helt faller utanför tillämpningsområdet för hemligheten i fråga om förtroliga meddelanden i 10 § i grundlagen. Det handlar alltså inte bara om en sådan omständighet som det hänvisas till i motiveringen till lagstiftningsordningen i den aktuella propositionen, det vill säga att ett sådant meddelande inte omfattas av kärnområdet i den rättighet som gäller sekretess i fråga om förtroliga meddelanden. Ett sådant meddelande åtnjuter inte skydd enligt 10 § 2 mom. i grundlagen, och bestämmelser om detta behöver inte bedömas utifrån de särskilda eller de allmänna förutsättningarna för inskränkning av de grundläggande fri- och rättigheterna enligt 10 § 4 mom. (GrUU 62/2024 rd, punkt 12). Således motsvarar även 70 § 3 mom. i den gällande lagen om militärunderrättelseverksamhet vad som grundlagsutskottet senare styrkt i sin praxis.

Grundlagsutskottet har i sin utlåtandepaxis (GrUB 4/2018 rd) betonat att regleringen i 10 § 4 mom. i grundlagen inte möjliggör allmän, oinriktad och allomfattande uppföljning av datatrafik i underrättelseverksamhet. Nödvändighetskriteriet i 10 § i grundlagen avser enligt utskottet å sin sida att en begränsning av hemligheten i fråga om förtroliga meddelanden är tillåten bara om det inte är möjligt att inhämta information genom mindre ingrepp, dels att informationsinhämtningen gör intrång på meddelandehemligheten så riktat och begränsat som möjligt. Utskottet har även i övrigt betonat betydelsen av förutsättningarna för att göra inskränkningar av de grundläggande fri- och rättigheterna då en ny begränsningsgrund tolkas.

Grundlagsutskottet har i sina utlåtanden om RP 203/2017 (GrUU 36/2018 rd. s. 24 och 76/2018 rd. s. 3) förutsatt att bestämmelser utfärdas om definitionen av sökbegrepp. Med grundlagsutskottets medverkan stiftades en definition av sökvillkor i lagen, enligt vilken sökbegrepp avser en uppgift som används för att vid underrättelseinhämtning som avser datatrafik så avgränsat och exakt som möjligt i en del av kommunikationsnätet selektera den datatrafik som är föremål för underrättelseinhämtningen, varvid intrånget i skyddet för hemligheten för förtroliga meddelanden sker endast i den omfattning som är nödvändig för att uppnå syftet med underrättelseinhämtningen.

I och med det gällande kategoriska förbudet att använda sökbegrepp som hänför sig till innehållet i ett meddelande, avgränsar inte den definition av sökbegrepp som föreskrivits med grundlagsutskottets medverkan inte alltid i första rummet information som inhämtats med underrättelseinhämtning som avser datatrafik till vad som är nödvändigt. Enligt 70 § i den gällande lagen får datatrafik enligt sökbegreppen behandlas automatiskt och manuellt, och det är även möjligt att rikta sökbegrepp som gäller meddelandets innehåll till datatrafik som inhämtas i det skedet. Även om en enskild myndighet inte i samband med den tekniska behandlingen av datatrafik enligt sökbegreppen egentligen sätter sig in i innehållet i meddelandena i datatrafiken, kan behandling av datatrafik enligt sökbegreppen överlag anses vara ett mer betydande ingrepp i skyddet för hemligheten i fråga om ett meddelande än att datatrafik avgränsas till datatrafik som motsvarar sökbegreppen (se även ovan i Europadomstolens mål Centrum för Rättvisa).

Det nu framlagda förslaget ger en möjlighet att använda språkliga sökbegrepp som hänför sig till meddelandets innehåll tillsammans med andra sökbegrepp (som redan för närvarande är tillåtna). Med det språkliga innehållet i ett meddelande avses i praktiken meddelandet

semantiska innehåll, det vill säga meddelandets betydelseinnehåll. Således är det möjligt att använda språkliga uttryck som sökbegrepp tillsammans med andra språkliga sökbegrepp än sådana som beskriver innehållet i meddelandet. Kombinationen av sökbegrepp avgränsar den datatrafik som inkommer till ett system för underrättelseinhämtning som avser datatrafik ännu noggrannare än tidigare, varvid det finns mindre datatrafik än tidigare i myndighetens manuella och automatiska behandling. Detta kan anses genomföra grundlagsutskottets krav på att underrättelseinhämtning som avser datatrafik ska riktas endast till vad som är nödvändigt på ett bättre sätt än i den gällande regleringen.

I propositionen föreslås även att ett sökbegrepp enligt den gällande regleringen (annat än språkligt sökbegrepp) kan finnas i meddelandet innehåll. Ett sådant sökbegrepp som avses i detta sammanhang kan anses rikta sig på ett noggrant sätt. Till exempel i en situation där det egentliga meddelandet inklusive förmedlingsinformation finns i ett annat meddelande (till exempel användning av en VPN-tunnel), hänför sig sökbegreppen på rätt sätt och till vad som är nödvändigt, även om sökbegreppet inte hänför sig till meddelandets yttersta skal. Å andra sidan kan ett sökbegrepp finnas i meddelandets innehåll i en situation där den anordning som används av objektet lagrar uppgifter, såsom kontaktuppgifter, i en molntjänst. Även i detta fall kan sökbegreppet anses hänföra sig till vad som är nödvändigt.

Sökbegrepp som definitionsmässigt beskriver innehållet i ett meddelande omfattas redan av den nuvarande definitionen av ett sökbegrepp, om sökbegreppet dock finns i innehållet i ett meddelande, ska kommunikationen utplånas utan dröjsmål.

Det nu behandlade förslaget kan anses vara proportionellt, eftersom onödig datatrafik kan raderas redan i det skede då datatrafik inhämtas på basis av användningen av sökbegrepp i datatrafiken. För närvarande kan militärunderrättelsemyndigheten efter inhämtandet av datatrafik enligt sökbegreppen behandla kommunikation automatiskt och manuellt, då även språkliga sökbegrepp kan riktas mot kommunikationen. I och med förslaget når mindre kommunikation militärunderrättelsemyndighetens fortsatta behandling och underrättelseinhämtningen från datatrafiken är således bättre riktad och avgränsad.

Den föreslagna ändringen kan bedömas ha konsekvenser som är positiva för de grundläggande fri- och rättigheterna, eftersom den avgränsar den mängd datatrafik som inkommer för att behandlas av militärunderrättelsemyndigheten och bättre än för närvarande genomför definitionen av sökbegreppet. Dessutom kan ingrepp i kommunikationen i det skede då sökbegrepp används inte anses vara ett lika betydande ingrepp i skyddet för privatlivet som att en tjänsteman från myndigheten behandlar och sätter sig in i innehållet i ett meddelande.

Sökbegrepp som hänför sig till en person eller teleterminalutrustning som finns i Finland

Enligt 68 och 70 § i lagförslag 1 i propositionen ändras bestämmelserna om underrättelseinhämtning som hänför sig datatrafik på så sätt att det absoluta förbudet att använda sökbegrepp som hänför sig till en person eller terminalutrustning som finns eller kan förmodas i Finland. I och med ändringen är det möjligt att använda sådana sökbegrepp tillfälligt. I praktiken avses med tillfällighet den tidsperiod under vilken det är möjligt att rikta noggrannare metoder för underrättelseinhämtning mot ett objekt som finns i Finland.

Grundlagsutskottet har inte uttryckligen tagit ställning till att man som sökbegrepp använder uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av en person som vistas i Finland eller som enligt förmodan används av honom eller henne. Grundlagsutskottet har i sin utlåtandepraxis (GrUB 4/2018 rd) betonat att regleringen i 10 § 4 mom. i grundlagen inte möjliggör allmän, oinriktad och allomfattande uppföljning av datatrafik

i underrättelseverksamhet. Nödvändighetskriteriet i 10 § i grundlagen avser enligt utskottet å sin sida att en begränsning av hemligheten i fråga om förtroliga meddelanden är tillåten bara om det inte är möjligt att inhämta information genom mindre ingrepp, dels att informationsinhämtningen gör intrång på meddelandehemligheten så riktat och begränsat som möjligt. Utskottet har även i övrigt betonat betydelsen av förutsättningarna för att göra inskränkningar av de grundläggande fri- och rättigheterna då en ny begränsningsgrund tolkas.

Den gällande lagen om militär underrättelseverksamhet ger inte möjlighet att använda information som fått från ett objekt som kommit till Finland, eftersom sådan information enligt 82 § 2 mom. i lagen ska utplånas utan dröjsmål och användningen av sökbegreppet ska avslutas.

I det nu behandlade förslaget till bestämmelse föreslås att man vid underrättelseinhämtning som avser datatrafik kan använda sökbegrepp som hänför sig till en person som tillfälligt vistas eller förmodas vistas i Finland samt hans eller hennes terminalutrustning. Sökbegrepp, som reglerats med grundlagsutskottets medverkan, avser en uppgift som används för att vid underrättelseinhämtning som avser datatrafik så avgränsat och exakt som möjligt i en del av kommunikationsnätet selektera den datatrafik som är föremål för underrättelseinhämtningen, varvid intrånget i skyddet för hemligheten i fråga om förtroliga meddelanden sker endast i den omfattning som är nödvändigt för att uppnå syftet med underrättelseinhämtningen. Ett sökbegrepp som i sig hänför sig till rätt objekt selekterar inte datatrafik beroende på var terminalutrustningen eventuellt finns.

Användningen av sökbegrepp som hänför sig till en person som vistas eller förmodas visas i Finland eller hans eller hennes teleterminalutrustning avgränsas till en viss tid. Användningen av sökbegrepp ska avslutas och man ska övergå till att använda en bättre riktad metod för underrättelseinhämtning så fort det i praktiken är möjligt. Detta uttrycks dock av förutsättningen enligt 70 § 1 mom. i lagen om att denna metod för underrättelseinhämtning kan användas endast om informationen inte kan skaffas med någon annan metod för underrättelseinhämtning. Nödvändighetskriteriet betonar för egen del tillgodoseendet av proportionalitetsprincipen och principen om ändamålsbundenhet i fråga om 68 och 70 § i lagen samt den sistahandskaraktär som föreskrivs i 70 § 1 mom.

Det bör observeras att ändringsförslaget inte kan anses möjliggöra att mer riktade underrättelsemetoder kringgås. Till andra delar är begränsningarna av underrättelseinhämtning som avser datatrafik fortfarande i kraft exempelvis i fråga om den interna datatrafik i Finland. Således är föremålet i varje fall datatrafik som är avsedd att överskrida Finlands gräns.

En militär aktör som kommer från andra sidan av Finlands gräns eller en aktör som allvarligt hotar den nationella säkerheten ska kunna identifieras och det ska vara möjligt att använda maximalt väl riktade metoder för underrättelseinhämtning mot objektet även då han eller hon kommer till det finska territoriet. I så fall är de uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av en person som vistas i Finland eller som han eller hon i övrigt använder noggranna och de hänför sig i enlighet med domstolstillståndet noggrant till en aktör som är föremål för militär underrättelseinhämtning.

De rättsobjekt som grundlagen skyddar, såsom den nationella säkerheten och Finlands suveränitet samt skyddet av människornas liv och hälsa, kan anses vara så betydande att det är befogat att undanröja förbudet att som sökbegrepp använda en teleterminalutrustning eller teleadress som innehas av en person som vistas i Finland eller som han eller hon i övrigt förmodas använda. I synnerhet i fråga om skyddet för Finlands suveränitet kan det anses vara betydelsefullt att information om att en statlig aktör kommer till Finland eller att en statlig aktör som finns i Finland kommunicerar med en aktör som på stadigvarande sätt befinner sig i

Finland. Således kan förslaget till bestämmelse anses ha även positiva konsekvenser för de grundläggande fri- och rättigheterna.

10.2.2.6 Rättsskydd

Enligt 21 § i grundlagen har var och en rätt att på behörigt sätt och utan ogrundat dröjsmål få sin sak behandlad av en domstol eller någon annan myndighet som är behörig enligt lag samt att få ett beslut som gäller hans eller hennes rättigheter och skyldigheter behandlat vid domstol eller något annat oavhängigt rättskipningsorgan. Offentligheten vid handläggningen, rätten att bli hörd, rätten att få motiverade beslut och rätten att söka ändring samt andra garantier för en rättvis rättegång och god förvaltning ska tryggas genom lag.

Grundlagsutskottet konstaterar i sitt betänkande om revideringen av de grundläggande fri- och rättigheterna att man vid begränsning av de grundläggande fri- och rättigheterna ska ombesörja tillräckliga rättsskyddsarrangemang (GrUU 25/1994 rd, s. 5). Med rättsskyddsarrangemang hänvisar man framför allt till möjligheten att söka ändring, men även andra processuella rättsskyddsgarantier kan bli aktuella.

Enligt artikel 13 i Europakonventionen, vilken gäller rätten till effektiva rättsmedel, 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.

I behandlingen av lagen om militär underrättelseverksamhet (GrUU 36/2018 rd) har grundlagsutskottet betonat starka rättsskyddsgarantier, omfattande och effektiv övervakning av användningen av underrättelsebefogenheter samt tillräckliga tillämpningsbegränsningar. Det rör sig om en exceptionell begränsningsgrund som inte bygger på att verksamheten ska vara brottslig och som således blir tillämplig också i fall där det inte går att peka på någon konkret och specificerad misstanke om brott varken i informationsinhämtningsfasen eller i övrigt (GrUB 4/2018 rd, s. 8).

På grund av syftet med underrättelseinhämtningen kan tillståndsförfarandet före den och övervakningen av genomförandet av underrättelseinhämtningen i allmänhet inte komma till underrättelseobjektets kännedom. Förfarandet i sig ger således skydd mot godtycke. Enligt utskottet framgår det av Europadomstolens praxis att rättslig kontroll i en domstol bäst tryggar kraven på att kontrollen ska vara självständig och opartisk (GrUU 36/2018 rd).

I fråga om metoderna för underrättelseinhämtning innebär fullgörandet av rättsskyddskraven särskilda utmaningar, eftersom objekten för befogenheterna inte kan förlita sig på de vanliga rättsskyddsmedlen i fråga om det egentliga beslutet om användning av en metod för underrättelseinhämtning. På grund av detta ska det finnas andra rättsskyddsarrangemang, med vilka en individs rättsskydd kan garanteras med tillräcklig säkerhet genom att på samma gång förebygga godtycke och missbruk av myndigheterna.

Inom underrättelseverksamhet har rättsskyddsarrangemangen och tillsynens effektivitet och lämplighet en accentuerad betydelse. 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 tilldela beslutsfattandet om användning av metoder för underrättelseinhämtning som innebär det allvarligaste ingreppet i skyddet för de grundläggande fri- och rättigheterna till en oberoende domstol (bland annat Weber och Saravia mot Tyskland). I fråga om underrättelseinhämtning som avser datatrafik kan underrättelsemyndigheterna inte heller ha direkt och obegränsat tillträde till datatrafiknät (Kennedy mot Förenade kungariket).

I Europadomstolens avgörandepraxis betonas även att myndigheten har det primära ansvaret för att verksamheten är lagenlig. Detta bidrar till att accentuera att befogenheter att begränsa de grundläggande fri- och rättigheterna tilldelas endast personer med tillräcklig utbildning och kompetens, vilket å sin sida accentueras i situationer där myndighetens beslut i princip inte underrättas till beslutsobjektet (GrUU 17/1998 rd, s. 2–3). Genom tillräcklig utbildning och kunskaper säkerställs även att man identifierar de normer som gäller grundläggande fri- och rättigheter och mänskliga rättigheter och förmågan att tillämpa dessa normer i den aktuella situationen.

Man har ansett att en annan sida av underrättelseskyldigheten är dess preventiva inverkan på myndighetsverksamhet. Med andra ord styr underrättelseskyldigheten myndigheterna att använda metoderna för underrättelseinhämtning i rätt omfattning och att förebygga missbruk, eftersom objektet i något skede blir medveten om underrättelseinhämtningen.

Underrättelsen har dessutom ansetts vara av betydelse med tanke på tillförlitligheten i användningen av metoderna för underrättelseinhämtning. En sammanslutning har ett allmänt intresse att övervaka att metoder för underrättelseinhämtning används inom ramen för godtagbara gränser.

I fråga om metoder för underrättelseinhämtning är det inte möjligt att utöva möjligheten att söka ändring eller underrättelseskyldigheten som en rättsskyddsgaranti. Det kan dock anses att detta kompenseras genom de andra tillsyns- och rättsskyddsarrangemangen. Dessa utgörs av en oberoende extern tillsyn (underrättelsetillsynsombudsmannen), som i omfattande grad övervakar verksamheten och användningen av metoder för underrättelseinhämtning i förskott, realtid och i efterskott. Beslut om metoder för underrättelseinhämtning som gör ett djupt intrång i de grundläggande fri- och rättigheterna fattas av domstol och de fakta som ska läggas fram i ett yrkande som lämnas till den har föreskrivits exakt genom lag. Utöver militärunderrättelsemyndighetens egen interna laglighetsövervakning övervakas militär underrättelseinhämtning av Försvarsmaktens assessor och försvarsministeriet. Även riksdagens justitieombudsman övervakar verksamheten.

Utöver det ovan konstaterade ska försvarsministeriet en gång per år tillstålla riksdagens underrättelsetillsynsutskott, riksdagens justitieombudsman och underrättelsetillsynsombudsmannen en berättelse om användningen av metoder för underrättelseinhämtning och skyddet av dessa.

I fråga om medborgare och enskilda personer är det signifikativt att de har rätt att framföra en begäran om undersökning (12 § i lagen om övervakning av underrättelseverksamheten) och klagomål (11 § i lagen om övervakning av underrättelseverksamheten) till underrättelsetillsynsombudsmannen.

Även om underrättelseskyldigheten i sig tryggar en individs möjligheter till rättsskydd och skapar transparens, kan man i fråga om hemlig myndighetsverksamhet anse att det framför allt handlar om ansvarsfullhet i verksamheten. Det handlar om huruvida tjänstemännen kan ställas inför rättsligt ansvar för eventuella försummelser. Så som konstaterats ovan, deltar flera

utomstående aktörer som är oberoende i förhållande till verksamheten och som ensamma och tillsammans även tillgodoser en enskild persons rättsskydd i övervakningen av militär underrättelseinhämtning. Dessutom utarbetas yrkanden och beslut hos militärunderrättelsemyndigheten av tjänstemän som genomgått en särskild utbildning och introduktion, förutsättningarna för användning av en metod för underrättelseinhämtning är noggrant reglerad och innehållet i yrkanden och beslut om användningen av metoder för underrättelseinhämtning är noggrant reglerat. En individ själv kan å sin sida framföra en begäran om undersökning eller klagomål till underrättelsetillsynsombudsmannen, även om han eller hon inte underrättats om användningen av en metod för underrättelseinhämtning.

Eftersom begäranden och klagomål till underrättelsetillsynsombudsmannen inte förutsätter en underrättelse som överlämnats till objektet eller den som blivit objekt, kan detta även anses kompensera underrättelseskyldighetens preventiva inverkan. Eftersom vem som helst kan framföra en begäran om undersökning eller klagomål, kan militärunderrättelsemyndigheten vara föremål för omfattande tillsyn även i fråga om medborgarna. Detta bidrar till att styra militärunderrättelsemyndigheten till noggrann tillämpning av lagen, så att en begäran om undersökning eller klagomål som gjorts till underrättelsetillsynsmyndigheten inte leder till fortsatta åtgärder. Underrättelsetillsynsombudsmannen kan hänskjuta ärendet för att utredas av förundersökningsmyndigheten och å andra sidan även avbryta eller avsluta användningen av en metod för underrättelseinhämtning, varvid ärendet även ska hänskjutas till en domstol för att avgöras. Ställande inför straffansvar och betalning av skadestånd orsakar så avsevärda risker för hela underrättelseverksamhet, såsom en risk för försämrat anseende och försämrat förtroende för militärunderrättelsemyndigheten, att även detta styr militärunderrättelsemyndigheten att förfara genom att noggrant iaktta lagen och att noggrant orientera och rikta verksamheten.

Personuppgifter behandlas vid underrättelseinhämtningen som helhet, varför den i fråga om rättsskyddet även kan bedömas ur denna synvinkel. Det finns bestämmelser om behandling av personuppgifter inom Försvarsmakten i den relevanta lagen om detta. Enligt den kan en person i enlighet med 29 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten begära att dataombudsmannen granskar personuppgifter och att behandlingen av dessa är lagenlig.

Även om ett objekt för underrättelseinhämtning inte ges någon underrättelse om den underrättelseinhämtning som avser datatrafik som objektet varit föremål för, kan systemet som helhet anses garantera de krav som ställs för rättsskyddet för en individ och myndighetens ansvar för de egna åtgärderna kan tillgodoses. Vid underrättelseinhämtning tillgodoses en individs rättsskydd som en samverkan av flera omständigheter.

De föreslagna bestämmelserna anses sålunda inte vara problematiska med tanke på 21 § i grundlagen.

10.2.3 De åtgärder som vidtas av en person utanför militärunderrättelsemyndigheten

10.2.3.1 En instans utanför myndigheten

Naturen på vidtagandet av en åtgärd

I 42 § 2 mom. i lagförslag 1 i regeringens proposition föreslås att även en aktör utanför myndigheten kan installera eller avinstallera en anordning, metod eller programvara enligt bestämmelsen. Den åtgärd som avses i bestämmelsen är avgränsad till installation och avinstallation. Den föreslagna regleringen är betydande med tanke på bestämmelserna i

grundlagen om rättsstatsprincipen i 2 § 3 mom., skyddet för privatlivet enligt 10 §, rättsskyddet i 21 §, tryggheten av de grundläggande fri- och rättigheterna i 22 § och bestämmelsen om överföring av en offentlig förvaltningsuppgift i 124 §.

Den föreslagna regleringen handlar om att fallspecifikt vidta åtgärder som omfattas av myndighetens befogenhet, där underrättelsemyndigheten inte själv har möjlighet att vidta en åtgärd som möjliggör användning av en metod för underrättelseinhämtning eller där vidtagandet av åtgärden kräver orimliga resurser i förhållande till de fördelar som kan fås. Det handlar om en situation som delvis liknar styrd användning av informationskällor. Styrd användning av informationskällor har reglerats med grundlagsutskottets medverkan (GrUU 66/2010 rd).

Vidtagandet av de föreslagna åtgärderna sker under myndighetens övervakning och styrning för att möjliggöra användningen av en metod för underrättelseinhämtning, om förutsättningarna för en egentlig metod för underrättelseinhämtning är uppfyllda och ett behörigt beslut fattats eller ett behörigt tillstånd fått för användningen av metoden för underrättelseinhämtning.

Med tanke på bedömningen av den föreslagna bestämmelsen kan det anses att det närmaste jämförelseobjektet i den gällande lagstiftningen utgörs av användning av informationskällor och i viss mån täckoperationer, via vilka förhållandet mellan förslaget till bestämmelse och grundlagen i viss mån kan bedömas. I fråga om bägge dessa bör det observeras att det nu behandlade förslaget till bestämmelse dock inte i regel förutsätter att personen infiltrerar sig i den verksamhet som utgör objekt.

I grundlagsutskottets utlåtandepraxis har användning av informationskällor hittills inte bedömts med tanke på de grundläggande fri- och rättigheterna. Bestämmelsen om användning av informationskällor ansågs vara behövlig med tanke på legalitetsprincipen för förvaltningen (RP 266/2004 rd s. 26). I propositionen föreslogs flera ändringar i polislagen, men grundlagsutskottet ansåg inte att det var behövligt att bedöma grundlagsenligheten uttryckligen för användning av informationskällor (GrUU 11/2005 rd). Bestämmelserna om användning av informationskällor har ändrats vid den övergripande revideringen av polislagen och tvångsmedelslagen (806/2011 och 872/2011). I grundlagsutskottets utlåtanden om propositionerna (GrUU 66/2010 rd och GrUU 67/2010 rd) ansåg man fortsättningsvis att det inte var behövligt att bedöma grundlagsenligheten. På motsvarande sätt bedömdes inte grundlagsenligheten för de bestämmelser som gäller användning av informationskällor i fråga om lagstiftningen om underrättelseverksamhet (GrUU 35/2018 rd och 36/2018 rd).

På samma sätt som i fråga om användning av informationskällor, baserar sig vidtagandet av de föreslagna åtgärderna i princip på personens tillträde till ett utrymme, en anordning eller ett informationssystem och personens befintliga kontakter, mänskliga relationer och vanliga umgänge. Vidtagandet av åtgärderna kan inte bedömas med tanke på begränsningen av skyddet för de grundläggande fri- och rättigheterna utifrån samma utgångspunkter som förtäckt inhämtande av information eller täckoperationer, eftersom åtgärderna inte handlar om infiltrering, utan om att utnyttjande av personens existerande tillträden och nätverk. En militärunderrättelsemyndighet har i princip inte motsvarande tillträde till dessa eller så kräver tillträdet att avsevärda resurser används. Såsom i fråga om användning av informationskällor ska den person som vidtar åtgärder kunna vidta åtgärder på ett sätt som motsvarar hans eller hennes normala verksamhet eller umgänge, eftersom verksamheten i annat fall i sista hand kan leda till en situation där personens liv och hälsa är äventyrade.

Användning av informationskällor anses inte handla om att det allmänna ingriper i en persons privatliv, utan om den inbördes relationen och det inbördes umgänget mellan individer samt om utnyttjande av detta för att bevaka det aktuella hotet. Vid vidtagandet av åtgärder kan det anses

handla om en motsvarande situation till den del som man i vidtagandet av åtgärden måste dra nytta av mänskliga relationer och mänskligt umgänge, vilket kan vara en förutsättning till exempel för att få tillträde till ett visst utrymme.

Det nu behandlade förslaget till bestämmelse kan anses innehålla även särdrag av täckoperationer. I fråga om brottsbekämpning har grundlagsutskottet karakteriserat täckoperationer som en okonventionell befogenhet, eftersom den ger myndigheten rätt att förfara i strid mot vissa straffrättsliga förbud utan tjänsteansvar. Enligt utskottets utlåtande kan legalitetsprincipen för förvaltningen anses innebära bland annat att en myndighet utan synnerligen vägande skäl och exakt definierade förutsättningar inte kan tilldelas nya former av befogenheter att vidta åtgärder, som i övrigt är straffrättsligt sanktionerade även om de vidtas av en myndighet (GrUU 5/1999 rd, s. 5). I propositionen föreslås att bestämmelser utfärdas om rätten för myndighetsexterna aktörer att vidta åtgärder, som beroende på situationen kan uppfylla rekvisitet för ett brott. De avsedda åtgärderna är dock sådana som myndigheten själv kan vidta utan att göra sig skyldig till ett brott.

Eftersom det handlar om en kompletterande åtgärd med koppling till användning av en metod för underrättelseinhämtning, är vidtagandet av åtgärden bundet till ett underrättelseuppdrag som baserar sig på objekten i 4 § i lagen om militär underrättelseverksamhet samt ett beslut eller tillstånd som gäller användningen av metoden för underrättelseinhämtning. I bestämmelsen om vidtagandet av åtgärderna finns det således inte något behov av att utfärda separata bestämmelser om vidtagande av åtgärderna på föremålen för militär underrättelseinhämtning på samma sätt som för vad som föreskrivits i fråga om styrd användning av informationskällor och täckoperationer.

Vidtagandet av en åtgärd handlar inte om infiltrering som är betydelsefullt med tanke på skyddet för privatlivet.

I och med vad som konstaterats ovan och därför att det handlar om verksamhet av osjälvständig natur, kan vidtagandet av åtgärden inte anses handla om verksamhet som det är befogat att bedöma på annat sätt än användning av informationskällor.

Den föreslagna regleringen anses inte, bedömt utifrån synpunkterna i systemet för de grundläggande fri- och rättigheterna, avvika från styrd användning av informationskällor, som föreskrivits med grundlagsutskottets medverkan (GrUU 66/2010 rd och GrUU 67/2010 rd). Utifrån vidtagandet av åtgärderna är det möjligt att rikta metoderna för underrättelseinhämtning på ett noggrannare sätt, utan att behöva göra någon föregående omfattande underrättelseinhämtning. Detta bedöms ha konsekvenser som är positiva för de grundläggande fri- och rättigheterna, då tiderna för och behovet av användning av andra metoder för underrättelseinhämtning, som kan innebära till och med en avsevärd inskränkning av de andra grundläggande fri- och rättigheterna, minskar.

Förhållandet till användning av offentlig makt

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 anförtros endast myndigheter.

Offentliga förvaltningsuppgifter hänvisar till en relativt vidsträckt helhet av administrativa uppgifter. Den omfattar uppgifter som hänför sig till bland annat verkställigheten av lagar samt

beslut om enskilda personers och sammanslutningars rättigheter, skyldigheter och förmåner (GrUU 8/2022 rd, s. 3–4).

Utgångspunkten i anknytning till en offentlig förvaltningsuppgift enligt 124 § i grundlagen är att tilldelande av sådana uppgifter till en privatperson inte får äventyra de grundläggande fri- och rättigheterna, rättsskyddet eller andra krav på god förvaltning (se till exempel GrUU 48/2001 rd, s. 3). I sin tolkningspraxis har grundlagsutskottet ansett att det för att kraven på rättssäkerhet och god förvaltning ska anses vara uppfyllda i den bemärkelse som avses i 124 § i grundlagen krävs att ärendena behandlas i enlighet med de allmänna förvaltningslagarna och att de som behandlar ärendena handlar under tjänsteansvar (GrUU 3/2009 rd, s. 4 och GrUU 20/2006 rd, s. 2).

I grundlagsutskottets utlåtandepraxis har man i flera sammanhang bedömt olika funktioner i förhållande till deras natur som offentliga förvaltningsuppgifter (se till exempel GrUU 26/2017 rd). I grundlagsutskottets praxis har man som skötsel av en offentlig förvaltningsuppgift betraktat bland annat lagstadgade social- och hälsovårdstjänster som tillhandahålls av privata serviceproducenter (GrUU 15/2018 rd), upprätthållande av ordningen och säkerheten (GrUU 20/2002 rd, s. 2), vaktverksamhet (GrUU 28/2001 rd, s. 5), myndighetsverksamhet genom inköpscentraler (GrUU 15/2019 rd), sjöräddningsväsendet (GrUU 24/2001 rd), lagstadgad arbetspensionsförsäkring (GrUU 45/1996 rd), rådgivning som omfattas av myndighetsansvar (GrUU 11/2006 rd) och avfallshanteringsuppgifter (GrUU 58/2010 rd).

Enligt förarbetena till revideringen av grundlagen har man som betydande utövning av offentlig makt betraktat till exempel rätt att använda maktmedel som grundar sig på självständig prövning eller att på annat sätt ingripa i individens grundläggande rättigheter (RP 1/1998 rd, s. 179/II, se även GrUU 28/2001 rd, s. 5–6). Grundlagsutskottet har i sin praxis ansett att granskningsbefogenheter som gäller intrång i hemfriden innebär en rätt att befatta sig i betydande grad med skyddet för hemfriden som tryggas för var och en i grundlagen och att en enskild person därmed inte kan få en sådan befogenhet genom en vanlig lag (se GrUU 40/2002 rd, s. 3/II och GrUU 46/2001 rd, s. 3/II).

Eftersom åtgärder som vidtas av en utomstående kan anses handla om åtgärder som ligger nära användning av informationskällor, kan förslaget till bestämmelse via denna synvinkel. I grundlagsutskottets utlåtandepraxis har man inte hittills bedömt användning av informationskällor med tanke på 124 § i grundlagen. I propositionen anser man att vidtagandet av åtgärder inte handlar om en offentlig förvaltningsuppgift som tilldelas en privatperson. Även om man i propositionen föreslår en möjlighet för en person utanför en militärunderrättelsemyndighet att vidta aktivare åtgärder än tidigare för att möjliggöra användning av en metod för underrättelseinhämtning, kan detta inte i fråga om natur anses avvika från användning av informationskällor på så sätt att vidtagandet av åtgärder ska bedömas som en offentlig förvaltningsuppgift enligt 124 § i grundlagen.

På samma sätt som i fråga om användning av informationskällor, kan möjligheten för en person utanför militärunderrättelsemyndigheten att vidta åtgärder för att möjliggöra användning av en metod för underrättelseinhämtning bedömas vara viktig. Tillträdet för en person till ett visst utrymme eller system kan bedömas ha rentav en avgörande roll för att genomföra underrättelseoperationen och för dess framgång och således även för hela Finlands försvar. Åtgärder som vidtas av utomstående handlar i princip om åtgärder som myndigheterna inte kan vidta genom att använda andra metoder eller en situation där användning av andra metoder i syfte att uppnå målet med underrättelseuppdraget inte är möjliga på grund av tids- eller resursrelaterade begränsningar. Det handlar alltså om att utnyttja möjligheter som en privatperson erbjuder och existerande möjligheter.

På motsvarande sätt som i fråga om användning av informationskällor, är den person som vidtar åtgärden delaktig i den verksamhet som utgör föremål för militär underrättelseinhämtning och han eller hon rör sig i utrymmen som anknyter till verksamhet och använder informationssystem i anknytning till den. På ett sätt som motsvarar användning av informationskällor, blir det förbjudet att använda en åtgärd, om den som vidtar åtgärden måste infiltrera sig i ett utrymme till vilket han eller hon inte har tillträde sedan tidigare, eller i verksamhet som han eller hon inte omfattas av sedan tidigare (RP 222/2010, s. 360). I dessa fall kan det anses handla om användningen av befogenhet till täckoperationer som hör till myndigheterna. Om en person på egen hand går med i viss verksamhet eller får tillträde till ett visst utrymme, handlar det å andra sidan inte om användning eller kringgående av täckoperationsbefogenheten.

Även om det nu behandlade förslaget till bestämmelse kan anses handla om aktivare verksamhet av en person utanför militärunderrättelsemyndigheten än i fråga om användning av informationskällor, blir de åtgärder som vidtas i situationer enligt den föreslagna bestämmelsen inte uppgifter av sådan natur att de ska bedömas som en offentlig förvaltningsuppgift. De åtgärder som vidtas baserar sig inte på självständig prövnings- eller beslutanderätt för personen. Personen gör inte heller som en del av verksamheten sådana avgöranden som påverkar privatpersoners rättigheter eller skyldigheter.

Vidtagandet av åtgärder handlar alltid om verksamhet som baserar sig på ett beslut och prövning av militärunderrättelsemyndigheten. Vidtagandet av åtgärder sker osjälvständigt inom noggrant fastställda ramar av militärunderrättelsemyndigheten samt utifrån dess anvisningar och under dess övervakning. Grunden för åtgärden utgörs alltid av ett beslut av en militärunderrättelsemyndighet om användning av en metod för underrättelseinhämtning och åtgärden vidtas i enlighet med beslutet av en person som i det specifika fallet har bedömts ha lämpliga egenskaper för att planmässigt vidta de exakt fastställda åtgärderna. En privatperson använder inte offentlig makt då han eller hon vidtar en åtgärd, utan det handlar uttryckligen om en befogenhet för militärunderrättelsemyndigheten, där användningen av metoden för underrättelseinhämtning är möjlig på grund av de åtgärder som vidtagits av privatpersonen.

De åtgärder som vidtas av en person utanför militärunderrättelsemyndigheten handlar i praktiken om stöd i anknytning till utövningen av militärunderrättelsemyndighetens befogenheter genom att utnyttja personens redan befintliga ställning i den verksamhet som utgör föremål för underrättelseinhämtningen. Åtgärderna är väldigt noggrant avgränsade och även till denna del av osjälvständig natur, då det handlar om till exempel att lämna en avlyssningsanordning på en viss på förhand fastställd plats. Det föreslås inte att en informationskälla ges rättigheter att använda befogenheter som hänför sig till kärnområdet för de grundläggande fri- och rättigheterna, utan det handlar på ovan konstaterade sätt endast om en myndighets befogenhet. Med beaktande av verksamhetens osjälvständiga natur anses den föreslagna regleringen inte heller till den här delen leda till att en förvaltningsuppgift tilldelas en privatperson.

Det bör observeras att militärunderrättelsemyndigheten inte har någon rätt att använda en metod för underrättelseinhämtning i ett utrymme som används för boende av permanent natur, och det är inte heller möjligt i en situation där en instans utanför myndigheten vidtar åtgärden.

Den föreslagna regleringen kan anses vara proportionell, eftersom delaktigheten i åtgärderna avgränsats endast till situationer där det är nödvändigt för att utöva den behöriga myndighetens befogenhet. I fråga om regleringens proportionalitet och rättsskyddsarrangemangen finns det skäl att observera att en person som inte är en myndighet inte kan användas för att kringgå förutsättningarna för och begränsningarna av användningen av befogenheter som tilldelats myndigheterna, utan beroende på situationen ska de förutsättningar som ställts på den

ifrågavarande metoden för underrättelseinhämtning alltid vara uppfyllda utan att det är inte möjligt att avvika från förfarandet med befogenhetsspecifikt beslutsfattande (Allan mot Förenade kungariket 5.11.2002, Van Vondel mot Nederländerna 25.10.2007, M.M. mot Nederländerna 8.4.2003 och A. mot Frankrike 23.11.1993).

Det kan vara nödvändigt att en informationskälla vidtar en åtgärd i situationer där informationskällan har tillgång till sådana utrymmen eller platser eller grupper till vilka förundersökningsmyndigheterna inte i övrigt av praktiska orsaker har tillgång, även om detta juridiskt sett vore tillåtet. Dessa åtgärder beträffande en informationskällas åtgärder föreskrivs med beaktande av regleringens syfte och regleringskontexten på ett tillräckligt exakt och noggrant avgränsat sätt i föreslagna 10 kap. 40 a § 3 mom. Förslaget effektiviserar möjligheterna att använda informationskällor och andra undersökningsmetoder och således i allmänhet utredningen av brott, vilket med tanke på systemet med grundläggande fri- och rättigheter kan ses som en godtagbar grund för att begränsa hemfridsskyddet.

I enlighet med det nu behandlade förslaget till bestämmelse har en aktör som inte hör till myndigheten inte någon rätt som baserar sig på självständig prövning att utöva en befogenhet som på avsevärt sätt ingriper i en individs grundläggande fri- och rättigheter. En sådan situation som avses i bestämmelsen handlar om installation eller avinstallation av ett föremål, en metod eller en programvara, det vill säga att en aktör utanför myndigheten utföra en teknisk åtgärd, som möjliggör att myndigheten utövar offentlig makt. Installationen eller avinstallationen ska utföras enligt myndighetens anvisningar. Den utomstående aktören har inte heller tillgång till eller närmare information om vilken information som skaffas från det egentliga objektet med föremålet, metoden eller programvaran.

Enligt det aktuella förslaget till bestämmelse installeras och avinstalleras ett föremål, en metod eller en programvara på begäran av en myndighet. Således kan den person som är föremål för en begäran även vägra att utföra åtgärden – verksamheten baserar sig på personens fria vilja och det handlar inte om en skyldighet.

10.2.3.2 De åtgärder som vidtas av Gränsbevakningsväsendet

Jämfört med den gällande lagen om militär underrättelseverksamhet föreskrivs som en ny bestämmelse i 18 a § i lagförslag 1 att Gränsbevakningsväsendet kan utföra en enskild åtgärd i anknytning till användning av vissa metoder för underrättelseinhämtning.

Förslaget är av betydelse med tanke på 2 § 3 mom. i grundlagen. Enligt det ska all utövning av offentlig makt bygga på lag. Grundlagsutskottet har i sitt utlåtande GrUU 35/2008 rd bedömt en motsvarande bestämmelse som ingick i regeringens proposition med förslag till lag om samarbete mellan polisen, tullen och gränsbevakningsväsendet och till vissa lagar som har samband med den (RP 26/2008 rd) och som gällde förfarandet för polisen, Tullen och Gränsbevakningsväsendet (PTG-myndigheterna) inom en annan PTG-myndighets uppgiftsområde. Enligt grundlagsutskottets utlåtande har utskottet flera gånger ansett att överföring av en offentlig behörighet som hänför sig till enskild person utifrån ett avtal från en myndighet till en annan inte är konstitutionellt ändamålsenligt (se till exempel GrUU 23/1994 rd, s. 2/I och GrUU 11/1994 rd, s. 1/II). Utskottet ansåg dock att det arrangemang som ingick i ovan nämnda lagförslag och som gäller PTG-myndigheternas samarbete krävs på grund av en ändamålsenligt användning av de olika myndigheternas resurser och att det även var konstitutionellt godtagbart.

Med hänvisning till sin tidigare praxis ansåg grundlagsutskottet dock att det var behövligt att precisera ordalydelsen i bestämmelserna så att de gäller endast en ”enskild” åtgärd i anknytning

till brottsbekämpning. På motsvarande sätt är det enligt utskottet behövligt att precisera ordalydelsen i fråga om omnämmandet om en brådskande åtgärd som vidtas utan begäran för att visa att även en annan PTG-myndighet i dessa fall får utöva endast de befogenheter som den har inom sitt eget uppgiftsområde.

Grundlagsutskottet har inte uttryckligen tagit ställning till hjälp som ges av en annan myndighet, där den myndighet som begär hjälp inte har befogenhet att vidta de aktuella åtgärderna (till exempel RP 82/2023, GrUU 36/2024 rd). Enligt förarbetena till revideringen av grundlagen har man i varje fall som betydande utövning av offentlig makt betraktat till exempel rätt att använda maktmedel som grundar sig på självständig prövning eller att på annat sätt ingripa i individens grundläggande rättigheter (RP 1/1998 rd, s 179/II, se även GrUU 28/2001 rd, s. 5–6).

Genom den föreslagna regleringen överförs inte uppgifter från en myndighet till en annan på ett sätt som är problematiskt med tanke på de grundläggande fri- och rättigheterna, utan en annan myndighet som redan har kunnande om vidtagande av den enskilda åtgärd som avses i bestämmelsen används för att utföra uppgiften. De metoder för underrättelseinhämtning som omfattar åtgärder som Gränsbevakningsväsendet kan vidta har begränsats till vissa enskilda metoder som omfattar motsvarande åtgärder som Gränsbevakningsväsendet redan kan vidta i fråga om förebyggande, förhindrande och avslöjande av brott i enlighet med lagen om gränsbevakningsväsendet. Genom åtgärderna är det inte heller tillåtet att utreda innehållet i ett meddelande. Dessutom ska de tjänstemän som utses för att utföra uppgifterna hos Gränsbevakningsväsendet ha tillräcklig utbildning för att klara av de åtgärder som föreslås i bestämmelsen.

Den föreslagna regleringen handlar om att fallspecifikt vidta åtgärder som omfattas av myndighetens befogenhet, i situationer där militärunderrättelsemyndigheten inte själv har möjlighet att vidta en åtgärd i anknytning till användning av en metod för underrättelseinhämtning eller där vidtagandet av åtgärderna kräver orimliga resurser. Dessutom har de åtgärder som vidtas en osjälvständig natur. I fallen enligt förslaget har myndigheten inte någon lagstadgad möjlighet att sätta sig in i det insamlade materialet, utan det ska överlämnas i obehandlad form för att behandlas av den myndighet som framfört begäran om handräckning.

Enligt 18 a § 2 mom. i lagförslag 1 i den nu behandlade propositionen kan Gränsbevakningsväsendet vidta åtgärder som avses i 28 § i gränsbevakningslagen på begäran av en militärunderrättelsemyndighet. Det handlar om vidtagande av åtgärder som omfattas av en annan myndighets befogenhet av en annan orsak än det ursprungliga användningsändamålet – militärunderrättelsemyndigheten har inte rätt att förordna att en gränskontroll ska genomföras. I förslaget till bestämmelse föreslås att uttryckliga bestämmelser utfärdas om en utvidgad användningsgrund.

Å andra sidan är det möjligt att konstatera att Gränsbevakningsväsendet med stöd av 28 § i gränsbevakningslagen kan utföra gränskontroller även utan någon brottsmisstanke. Gränsövervakningen kan anses avse verksamhet vid de internationella gränserna, vars syfte är att upprätthålla fredliga förhållanden, trygga den territoriella integriteten och förhindra olagliga gränspasseringar. Således kan förslaget inte anses avsevärt utvidga användningen av Gränsbevakningsväsendets befogenheter. I 3 § i lagförslag 1 i propositionen föreslås att deltagande i militär underrättelseinhämtning föreskrivs som en uppgift för Gränsbevakningsväsendet.

Bestämmelserna i 18 a § i lagförslag 1 i regeringspropositionen krävs på grund av en ändamålsenlig användning av myndigheternas resurser och de ligger således i linje med grundlagsutskottets ståndpunkt. Bestämmelsen kan anses vara konstitutionellt godtagbar.

Bestämmelsen kan anses vara exakt i fråga om när en annan myndighet kan vidta åtgärder. Eftersom militärunderrättelsemyndigheten har ansvaret, är åtgärderna dessutom föremål för kraftig tillsyn.

10.2.4 Teknisk observation av utrustning

I anknytning till teknisk observation av utrustning föreslås i propositionen att ett tillstånd för teknisk observation av utrustning inte framöver längre ansöks och beviljas för vissa specificerade anordningar eller programvaror, utan att domstolen bedömer om teknisk observation av utrustning kan riktas mot en anordning eller programvara som används av en person med anknytning till ett visst föremål för militär underrättelseinhämtning. Utredning av de anordningar och programvaror som använts av den misstänkte förblir ett ärende som ska utredas av en tjänsteman från militärunderrättelsemyndigheten under tjänsteansvar. Tjänstemannen ska fatta ett särskilt beslut om de anordningar och programvaror som är föremål för åtgärden, i vilket skälen för valet av de anordningar och programvaror som utgör föremål för åtgärden uttryckligen ska motiveras.

Lagförslaget handlar om en ny typ av regleringslösning, och polislagen eller tvångsmedelslagen innehåller inte någon motsvarande reglering.

Med tanke på den nu behandlade bedömningen är den begränsning av de grundläggande fri- och rättigheterna som följer av teknisk observation av utrustning relevant, i och med att den hänför sig till skyddet för privatlivet och i viss mån till skyddet för ett förtroligt meddelande. Ur denna synvinkel har antalet anordningar eller programvaror som används av den person som utgör objekt eller antalet tillstånd för dem inte någon avgörande betydelse. Det relevanta är däremot om det är möjligt att begränsa skyddet för privatlivet eller för ett förtroligt meddelande för en person med koppling till föremålet för militär underrättelseinhämtning genom teknisk observation av utrustning som riktas på en anordning eller programvara som han eller hon använder. Förslaget har likheter med teleavlyssning, som med grundlagsutskottets medverkan (GrUU 35/2018 rd och GrUU 36/2018 rd) föreskrivits i 5 a kap. i polislagen och 4 kap. i lagen om militär underrättelseverksamhet. Enligt den föreslagna regleringen ska dessutom ett ovan beskrivet motiverat beslut fattas om inriktningen av teknisk observation av utrustning.

Ett tillstånd till teknisk observation av utrustning som hänför sig till en person är i kraft i tre månader, varefter ärendet ska hänskjutas till tillståndsprövning på nytt. Även de nya anordningar och programvaror som en person använder ska läggas fram i den nya prövningen.

Grundlagsutskottet har tagit ställning till riktande av teleavlyssning mot en person med avseende på ändringen av tvångsmedelslagen (RP 217/2022 rd, GrUU 98/2022 rd). Grundlagsutskottet har redan innan ikraftträdandet för revideringen av de grundläggande fri- och rättigheterna ansett att en väsentlig fråga som gäller rättsskyddet är att förutsättningen för en befogenhet för teleavlyssning alltid är oberoende av det tillstånd som en domstol gett i det enskilda fallet med anledning av en konkret brottsmisstanke (GrUU 8/1994 rd, s. 2/II). I sin senare praxis har utskottet bland annat förkastat förslaget till att möjliggöra teleavlyssning kortvarigt utan domstollstånd (GrUU 66/2010 rd, s. 10—11). Utskottet har dessutom ansett att det är befogat att överväga att befogenheten att ge avgöranden även i fråga om andra hemliga tvångsmedel tilldelas domstolarna (GrUU 66/2010 rd, s. 9/II). Grundlagsutskottet har som sin uppfattning konstaterat att ändringen av tvångsmedelslagen är ägnad åt att försämma rättsskyddet i fråga om användningen av teletvångsmedel.

Det föreslås att man till 33 § i lagförslag 1 i propositionen fogar en bestämmelse om beslutsfattande i en situation där teknisk observation av utrustning hänför sig till en person och

en ny anordning eller programvara fogas till användningen av en metod för underrättelseinhämtning. En motsvarande ändring görs beträffande teleavlyssning (36 §) i fråga om en ny teleadress eller teleterminalutrustning.

På samma gång fogas i anknytning till användning av ovan avsedda metoder för underrättelseinhämtning nya 82 a § till lagen om militär underrättelseverksamhet, som gäller avbrytande av teleavlyssning och användning av vissa andra metoder för underrättelsemetoder, om det kommer fram att teleavlyssningen hänför sig till ett annat meddelande som än ett sådant som sänds av eller är avsett för den som är föremål för tillståndet. På motsvarande sätt ska man i fråga om teknisk observation av utrustning avbryta användningen av en metod för underrättelseinhämtning, om det kommer fram att användningen av en metod för underrättelseinhämtning hänför sig till någon annan anordning eller programvara än den som objektet använder.

Med tanke på det nu behandlade förslaget till bestämmelse är det centralt att militärunderrättelsemyndighetens verksamhet övervakas av en extern övervakare (underrättelsetillsynsombudsmannen) i förväg, i realtid och i efterskott. Övervakningen i realtid garanteras för egen del militärunderrättelsemyndighetens skyldighet att göra en anmälan till ombudsmannen om ett beslut om användning av en metod för underrättelseinhämtning. Enligt det nu behandlade förslaget fattar militärunderrättelsemyndigheten alltid beslut om fogande av en ny anordning eller programvara för att omfattas av tillståndet. Således omfattas även nya anordningar och programvaror av den externa laglighetsövervakningen, fram till dess att ett eventuellt fortsatt tillstånd för teknisk observation av utrustning ansöks från den domstol.

Underrättelsetillsynsombudsmannen har rätt att avbryta eller avsluta användningen av underrättelsemetoden, om han eller hon anser att tillsynsobjektet förfarit i strid med lagen i underrättelseverksamheten. Ombudsmannen har möjlighet att ge ett temporärt förordnande om en metod för underrättelseinhämtning som prövas av en domstol och ärendet ska hänskjutas till domstol. Även om militärunderrättelsemyndigheten inte själv fattar beslutet om att foga en anordning eller programvara till tillståndet för teknisk observation av utrustning, övervakar underrättelsetillsynsombudsmannen således detta och ombudsmannen kan vid behov ingripa i ärendet.

På grund av de nämnda orsakerna ska förslaget inte anses vara problematiskt med tanke på skyddet för de grundläggande fri- och rättigheterna.

10.2.5 Användningen av en utomstående anordningar eller informationssystem

I lagförslag 1 i propositionen är 42 § 3 mom. relevant med tanke på 15 § i grundlagen. Enligt 15 § 1 mom. i grundlagen är vars och ens egendom tryggad.

Grundlagsutskottet har i sin vedertagna utlåtandepraxis konstaterat att det till exempel i fråga om Försvarsmaktens rätt att tillfälligt använda fastigheter, med tanke på det egendomsskydd som tryggats i 15 § i grundlagen, finns ett vägande samhälleligt behov i anknytning till det militära landsförsvaret. Behoven av militär övningsverksamhet och höjning av försvarsberedskapen är med tanke på systemet för de grundläggande fri- och rättigheterna godtagbara grunder för att begränsa egendomsskyddet. Tillfällig användning av en fastighet förutsätts vara nödvändigt för de funktioner som nämns i bestämmelsen (till exempel GrUU 51/2006 rd, s. 5).

Grundlagsutskottet har inte tagit ställning till någon helt motsvarande situation som det handlar om i det nu behandlade förslaget till bestämmelse.

Enligt det nu behandlade förslaget till bestämmelse kan en militärunderrättelsemyndighet använda en utomståendes anordning eller datasystem, om det är nödvändigt för att installera och avinstallera en metod eller en programvara eller för att ta emot uppgifter som skaffas genom metoden eller programvaran. I enlighet med bestämmelsen får den utomstående eller dennes anordning eller datasystem inte orsakas onödig skada av användningen för detta syfte. Användningen ska även tidsmässigt avgränsas till vad som är nödvändigt och en enskild anordning eller ett enskilt datasystem får i princip användas endast i den nödvändiga tiden, till exempel för att överföra ett enskilt datatekniskt kommando till objektet för underrättelseinhämtning. När uppgifter tas hem från objektet ska man på motsvarande sätt bedöma om uppgifterna ska tas hem via flera olika anordningar och datasystem.

Det står i sig klart att en militärunderrättelsemyndighet inte kan skaffa information om andra uppgifter som ingår i en anordning eller ett datasystem som utgör förmedlare eller som går via sådana.

Förslaget till bestämmelse är nödvändigt för att kunna få information om verksamheten hos den som är objekt för militär underrättelseinhämtning. Militärunderrättelsemyndigheten har inte i alla situationer möjlighet att i smyg utföra de åtgärder som avses i förslaget till bestämmelse. En förutsättning för att vidta åtgärden är att den är nödvändig, det vill säga att åtgärden i praktiken inte kan vidtas med andra metoder.

En tillfällig begränsning av egendomsskyddet är nödvändig för att uppnå ett godtagbart mål, det vill säga i sista hand att trygga Finlands suveränitet och skydda den nationella säkerheten. Det bedöms att inskränkningen av de grundläggande fri- och rättigheterna är liten.

10.2.6 Omhändertagande och provtagning från ett ämne, egendom eller ett föremål

Det tillfälliga omhändertagandet av ämnen, egendom eller föremål vilket föreslås i 56 a § i lagförslaget 1 i propositionen gäller situationer där användning av befogenheten till provtagning enligt föreslagna 55 a § i lagen eller kopiering enligt 56 § inte nödvändigtvis förutsätter att militärunderrättelsemyndigheten har rätt att tillfälligt omhänderta ett ämne, egendom eller ett föremål. Ämnet, egendomen eller föremålet ska utan dröjsmål återlämnas när syftet med omhändertagandet har uppnåtts. Förfarandet enligt föreslagna 56 a § motsvarar det förfarande som föreskrivs i 7 kap. 8 § 1 mom. i tvångsmedelslagen, men den centrala skillnaden är att befogenheten inte är avsedd att utövas vid ett omhändertagande som pågår i en längre tid. Med beaktande av underrättelseverksamhetens natur ska man dessutom sträva efter att returnera ett ämne, ett föremål eller egendom till läget vid tidpunkten för omhändertagandet i en så oförändrad form som omöjligt, så att underrättelseverksamheten inte avslöjas.

Förslaget till bestämmelse gäller 15 § 1 mom. i grundlagen, vilket skyddar rätten för ägaren att besitta, använda och utnyttja sin egendom, såsom sina föremål och handlingar, på önskat sätt samt rätten att bestämma över dessa.

Ett omhändertagande med stöd av 56 a § i lagförslag 1 i propositionen innebär att man tillfälligt begränsar nyttjanderätten och bestämmanderätten för ägaren av ett föremål, ett ämne eller egendom. Den föreslagna regleringen i 56 a § kan dock anses vara godtagbar med tanke på den helhet som utgörs av systemet med grundläggande fri- och rättigheter och krävas av ett vägande samhälleligt behov, eftersom militärunderrättelsemyndigheten genom att utöva befogenheten kan säkerställa att de uppgifter som föreskrivits för den genom lag sköts på behörigt sätt, till exempel genom att granska sammansättningen av ett ämne som finns i aktörens utrymmen. Föremålet för åtgärden är ämnen, föremål eller egendom som kan användas tillsammans eller separat för att skada människor eller ämnen, egendom eller föremål vars innehav redan i princip

förbjudits annanstans i lagstiftningen. Sådana lagar kan vara till exempel skjutvapenlagen (1/1998) och kemikalielagen (599/2013). Även ordningslagen (612/2003) förbjuder helt att vissa ämnen och föremål innehåsas på en allmän plats (9 §). I en situation enligt det nu behandlade förslaget handlar det dock inte om situationer av ringa betydelse.

Inskränkningen av egendomsskyddet begränsas av att militär underrättelseverksamhet i princip äger rum i hemlighet för dess föremål och att man försöker hindra att åtgärderna avslöjas så länge som möjligt. Dessutom begränsas omfattningen av inskränkningen av de principer som föreskrivs i lagen om militär underrättelseverksamhet, i synnerhet principen om minsta olägenhet, som regleras i 7 § i lagen. Enligt den får man genom användningen av befogenheten för militär underrättelseinhämtning 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. Utifrån det ovan avsedda begränsar sig provtagningen de facto och juridiskt sett till en liten mängd egendom som är föremål för metoden, i praktiken till en så liten del som inte kan upptäckas med blotta ögat.

Vid underrättelse om utövning av befogenheten tillämpas bestämmelserna om underrättelseskylldigheten. Så som i fråga om andra metoder för underrättelseinhämtning kan en person vars ämne, föremål eller egendom blivit föremål för utövning av befogenheten, göra en begäran om undersökning eller framföra klagomål till underrättelsetillsynsombudsmannen, oberoende av om han eller hon fått ett meddelande om eller har motiverade skäl att misstänka att han eller hon blivit föremål för användning av en metod för underrättelseinhämtning. Det bedöms att inskränkningen av de grundläggande fri- och rättigheterna är liten.

En tillfällig begränsning av egendomsskyddet är nödvändig för att uppnå ett godtagbart mål, det vill säga i sista hand att trygga Finlands suveränitet och skydda den nationella säkerheten.

10.2.7 Värnpliktiga och andra som deltar i en övning

De förslag till bestämmelser som gäller internationellt samarbete (20 § i lagförslag 1), deltagande i militär underrättelseinhämtning av personer i en tjänst enligt värnpliktslagen eller personer som deltar i en frivillig övning (91 § i lagförslag 1) och installation och avinstallation av anordningar, metoder eller programvara (42 § i lagförslag 1) ska bedömas med tanke på grundlagens reglering om tilldelning av en förvaltningsuppgift till någon annan än en myndighet.

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 anförtros endast myndigheter (RP 1/1998 rd, s. 179).

Inga principiella rättsliga begränsningar har ställts på att använda beväringar och andra värnpliktiga som är i en tjänst eller deltar i en övning i en tjänst som baserar sig på skyldigheten att försvara landet enligt 127 § i grundlagen.

Vid reservens repetitionsövningar upprätthålls den militära kunskap och förmåga som inhämtats under beväringstjänsten samt ges utbildning för mera krävande uppgifter.

När en person som deltar i en övning biträder en militärunderrättelsemyndighet har han eller hon med stöd av 91 § rätt att utöva befogenheter endast under uppsikt och övervakning av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman. Den

som deltar i en övning beslutar inte om användningen av en metod för underrättelseinhämtning eller om hur användningen av en metod för underrättelseinhämtning riktas. De metoder för underrättelseinhämtning som står till deras förfogande föreskrivs uttryckligen.

Den som deltar i en övning ska ha kunskap och kunnande för att sköta uppgiften. 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 kan inte anses handla om användning av självständig beslutanderätt eller avsevärd utövning av offentlig makt.

10.2.8 Underrättelseinhämtning som hänför sig till en statlig aktörs datasystem i hemlandet

I 61 a § i lagförslag 1 i propositionen föreslås att man utfärdar bestämmelser om underrättelseinhämtning i hemlandet som avser statliga aktörers datasystem. De programvaror och anordningar som hör till informationssystemet kan vara föremål för användningen av en metod för underrättelseinhämtning.

I regerings proposition om ändring av 10 § i grundlagen (RP 198/2017 rd) har det konstaterats att en främmande stats myndighetsorganisation inte åtnjuter skydd för hemligheten i fråga om förtroliga meddelanden. I sitt betänkande om ändringen (GrUB 4/2018 rd) konstaterade grundlagsutskottet att även om en främmande stats militär- eller en annan myndighetsorganisations kommunikation inte åtnjuter skyddet för hemligheten i fråga om förtroliga meddelanden, kan befogenheter till militärunderrättelseinhämtning i samtliga fall inte riktas så exakt att det inte finns någon fara för att myndigheterna tillfälligt får tillgång till uppgifter om kommunikationen för enskilda personer utan koppling till underrättelseuppdraget, vilket enligt grundlagsutskottets mening ska avgränsas till en så liten omfattning som möjligt i vanliga lagar.

Grundlagsutskottet lade fram centrala grunder som ska beaktas i bedömningen av militär verksamhet och annan verksamhet som allvarligt hotar den nationella säkerheten enligt 10 § 4 mom. i grundlagen, vilka utgör en grund för att begränsa hemligheten i fråga om förtroliga meddelanden. Utskottet betonade starka rättsskyddsgarantier, omfattande och effektiv övervakning av användningen av befogenheter till underrättelseinhämtning samt tillräckliga tillämpningsbegränsningar. Det rör sig om en exceptionell begränsningsgrund som inte bygger på att verksamheten ska vara brottslig och som således blir tillämplig också i fall där det inte går att peka på någon konkret och specificerad misstanke om brott varken i informationsinhämtningsfasen eller i övrigt (GrUB 4/2018 rd, s. 8). Även med beaktande av underrättelseinhämtningens avvikande natur i förhållande till brottsbekämpning och brottsutredning har den regleringsmodell som tillägnats i lagstiftningen om underrättelseinhämtning enligt grundlagsutskottet inte kunnat användas som motivering till den föreslagna regleringen kring underrättelseinhämtning (GrUU 99/2022 rd).

Vid riksdagsbehandlingen av lagen om militär underrättelseinhämtning har utskottet i fråga om befogenheterna betonat att bestämmelsens tillämpningsområde på det sätt som beskrivs i motiveringarna till regeringens proposition (RP 203/2017 rd) hänför sig till inhämtande av information endast i fråga om militär verksamhet som riktar sig mot Finland eller till militär verksamhet som är av betydelse för den finländska säkerhetsmiljön. Utskottet har betonat behovet av att tolka en begränsningsgrund snävt (GrUB 4/2018 rd, s. 7). Utskottet har även betonat betydelsen av de allmänna förutsättningarna för att begränsa de grundläggande fri- och rättigheterna då begränsningsgrunden enligt 10 § tolkas (GrUB 4/2018 rd, s. 8–9).

I egenskap av metod för underrättelseinhämtning handlar den i 61 a § i lagförslag 1 föreslagna bestämmelsen om en befogenhet som kombinerar åtgärder inom teleavlyssning, teleövervakning, teknisk observation av utrustning och teknisk avlyssning. Alla ovan avsedda enskilda metoder för underrättelseinhämtning har bedömts grundligt i grundlagsutskottets utlåtandepraxis.

Det nu behandlade förslaget kan delvis bedömas visavi teleavlyssning och teleövervakning mot en person, vilken redan för närvarande är tillåten, samt teknisk observation av utrustning mot en person vilken föreslås i denna proposition. Det handlar dock om en statlig aktör och att information inhämtas från den helhet som utgörs av de anordningar, programvaror och datatrafikförbindelser som den använder.

Den inskränkning av de grundläggande fri- och rättigheterna vilken hänför sig till skyddet för förtrolig kommunikation och orsakas av den nya befogenheten är relevant med tanke på den aktuella bedömningen. Så som konstaterats ovan åtnjuter en statlig aktörs kommunikation inte något motsvarande skydd för de grundläggande fri- och rättigheterna som privata personer. Således är det med tanke på bedömningen centralt i vilken mån användningen av den nya befogenheten omfattar annan kommunikation än sådan kommunikation av statlig aktör vilken utgör föremål för underrättelseinhämtningen. Det avgörande är inte antalet anordningar, programvaror, teleterminalutrustningar och teleadresser vilka den statliga aktören använder eller det antal befogenhetstillstånd som hänför sig till dessa. Det väsentliga är om det är möjligt att begränsa skyddet för förtrolig kommunikation för enskilda personer som eventuellt behandlas i objektet.

Grundlagsutskottet har redan innan ikraftträdandet för revideringen av de grundläggande fri- och rättigheterna ansett att en väsentlig fråga som gäller rättsskyddet exempelvis är att förutsättningen för en befogenhet för teleavlyssning alltid är oberoende av det tillstånd som en domstolen gett i det enskilda fallet med anledning av en konkret brottsmisstanke (GrUU 8/1994 rd, s. 2/II).

Förutsättningarna för användning av den nya befogenhet som föreslås i denna regeringsproposition motsvarar vad som även i övrigt föreskrivits i fråga om befogenheter som avsevärt ingriper i skyddet för andra grundläggande fri- och rättigheter. Dessutom utgörs föremålet för användning av befogenheten för objekt som föreskrivits separat i lagen och i fråga om dessa en statlig aktör som föreskrivits i lagen.

Nivån på beslutsfattandet eller förutsättningarna för användning avviker inte i förhållande till vad som föreskrivits om teleavlyssning och teleövervakning eller teknisk observation av utrustning mot en person enligt vad som föreslås i denna proposition. Det handlar om ändring av nivån på beslutsfattandet i ett ärende där en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman redan för närvarande har en stark ställning. I fråga om den föreslagna nya befogenheten finns det skäl att betona att enligt den föreslagna regleringen ska en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman fatta ett beslut om anordningar, programvaror, teleterminalutrustningar och teleadresser vilka är föremål för en åtgärd i den datasystemhelhet som fastställts i domstolstillståndet, i vilket man uttryckligen ska motivera orsakerna till att de valts, det vill säga varför objektet är en del av det informationssystem som avses i beslutet. Redan för närvarande är motiveringsskyldigheten hög i fråga om andra metoder för underrättelseinhämtning och beslutet är föremål för stark laglighetsövervakning.

Utredningen av identifieringsuppgifter om anordningar, programvaror, teleterminalutrustningar och teleadresser vilka används av en statlig aktör i en viss informationssystemhelhet förblir ett ärende som ska skötas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Vid verksamhet som avses i bestämmelsen kan dock även en utomstående kommunikation omfattas av underrättelseinhämtningen. I 85 § i lagförslag 1 i propositionen föreskrivs att underrättelseinhämtning som avser en statlig aktörs informationssystem i Finland ska avbrytas och att de uppgifter som inhämtats med metoden ska utplånas direkt, om man med den får andra uppgifter än uppgifter som behandlas i en statlig aktörs informationssystem.

Beslutet om användning av metoden för underrättelseinhämtning fattas av en domstol. I 61 b § i lagförslag 1 i propositionen finns det exakta bestämmelser om förutsättningarna och om de omständigheter som ska nämnas såväl i ett yrkande som i ett beslut om tillstånd. Eftersom det kan anses handla om en befogenhet som kombinerar åtgärder som redan är lagstadgade, vars föremål, som utgörs av en statlig aktörs informationssystemhelhet, utifrån de uppgifter som fås under användningen av en metod för underrättelseinhämtning kan ändras under giltighetstiden för ett tillståndet, fattas beslutet om en anordning, programvara, teleterminalutrustning eller teaddress med anknytning till det informationssystem som utgör föremål för ett beslut om användning av en metod för underrättelseinhämtning enligt föreslagna 61 b § av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. Ett i beslutet avsett informationssystem eller en del i det ska inkluderas i ett nytt tillståndskrav som möjliggör användning av en metod för underrättelseinhämtning.

Användningen av befogenheten är föremål för den kraftiga externa övervakningen av underrättelsetillsynsombudsmannen. Så som konstaterats tidigare har en militärunderrättelsemyndighet en skyldighet att anmäla sina beslut till underrättelsetillsynsombudsmannen. Således görs en anmälan om beslut om nya anordningar, programvaror, teleterminalutrustningar och teleadresser som omfattas av ett tillstånd som en domstol beviljat till underrättelsetillsynsombudsmannen på samma sätt som exempelvis i fråga om teleavlyssning mot en person. Underrättelsetillsynsombudsmannen övervakar att nya anordningar, programvaror, teleterminalutrustningar och teleadresser finns i den datasystemhelhet som avses i det tillstånd som beviljats av en domstol.

Förslaget till bestämmelse kan anses vara problemfritt med tanke på grundlagen. Förslaget förbättrar möjligheterna för en militärunderrättelsemyndighet att inhämta information om en statlig aktör, vilket i sista hand möjliggör att man kan skydda personernas liv och hälsa och förbättra säkerheten i samhället. Dessutom kan regleringen anses ha positiva konsekvenser för de grundläggande fri- och rättigheterna.

10.2.9 Deltagande av en utländsk tjänsteman i militär underrättelseinhämtning

Den föreslagna regleringen i 20 § i lagförslag 1 beträffande deltagande av en utländsk tjänsteman i användningen av en metod för underrättelseinhämtning på finskt territorium är relevant med tanke på Finlands suveränitet enligt 1 § i grundlagen.

Enligt 1 § 1 mom. i grundlagen är Finland en suverän republik. Enligt 1 § 3 mom. i grundlagen deltar Finland i internationellt samarbete i syfte att säkerställa fred och mänskliga rättigheter samt i syfte att utveckla samhället. Finland är medlem i Europeiska unionen och hör till Nordatlantiska fördragsorganisationen.

I förarbetena till grundlagen konstateras dessutom att: ”Statens suveränitet omfattar både den inre och den yttre suveräniteten. Med inre suveränitet avses att statsmakten utgör den högsta rättsliga makten i staten. Den viktigaste konsekvensen av den inre suveräniteten är behörigheten att bestämma om de myndigheters och andra organs behörighet som utövar offentlig makt inom statens territorium. Behörigheten omfattar även makt att besluta om rättsordningens innehåll, bestämma om de statliga organens verksamhet och rätt att på olika sätt utöva offentlig makt i förhållande till människor och föremål inom statens territorium. Med yttre suveränitet avses statens frihet att självständigt besluta om sina förhållanden till andra stater och till internationella organisationer.” (RP 1/1998 rd, s. 73). Finland har även ingått bilaterala avtal som försvarssamarbete, av vilka det avtal som försvarssamarbete som ingåtts med Förenta staterna är det centrala.

Av betydelse med tanke på bedömningen av suveräniteten är framför allt att en främmande stats och dess tjänstemans verksamhet grundar sig på ett beslut av finska myndigheter (se även GrUU 66/2016 rd, s. 3 och GrUU 65/2016 rd, s. 3). Metoder för underrättelseinhämtning används enligt bestämmelsen i 20 § i lagförslag 1 under styrning och övervakning av en militärunderrättelseverksamhet. Dessutom är en utländsk tjänsteman skyldig att iakttä föreskrifter, begränsningar och anvisningar som militärunderrättelsemyndigheten gett honom eller henne.

Enligt förarbetena till grundlagen och grundlagsutskottets praxis ska man som betydande utövning av offentlig makt betrakta till exempel rätt att använda maktmedel som grundar sig på självständig prövning eller att på annat sätt ingripa i individens grundläggande fri- och rättigheter. Det föreslås att 20 § i lagen om militär underrättelseverksamhet innehåller bestämmelser om deltagande av en utländsk behörig tjänsteman i användningen av metoder för underrättelseinhämtning utan närmare avgränsning av metoderna. Beslutsfattandet om internationellt bistånd och begäran om sådant föreskrivs separat i den relevanta lagen om detta (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. Deltagandet i användningen av metoder för underrättelseinhämtning hålls således alltid under styrning och tillsyn av en finländsk tjänsteman. Dessutom står det klart att en tjänsteman från en främmande stat vid förfarande i Finland omfattas av det straff- och skadeståndsrättsliga ansvaret. Militärunderrättelseinhämtningen ansvarar även för de behövliga tillstånden.

På grund av dessa förfarandegarantier och ansvarsarrangemang bedöms den föreslagna paragrafen inte vara problematisk i förhållande till kravet enligt 124 § i grundlagen på att uppgifter som i avsevärd grad innehåller utövning av offentligt makt kan anförtros endast myndigheter.

Deltagandet täcker även att en utländsk tjänsteman kan delta i analysen av de inhämtande uppgifterna. Enligt 111 § i den gällande lagen kan bland annat huvudstabens underrättelsechef ge ett förordnade utifrån vilket en expert kan undersöka upptagningar. I och med den nu behandlade ändringen kan en utländsk tjänsteman delta i undersökningen av upptagningar utan uttryckligt beslut. Beslutet fattas alltså i det skede då beslutet om att en utländsk tjänsteman ska komma till Finland fattas och han eller hon ges föreskrifter, begränsningar och anvisningar.

De föreslagna bestämmelserna anses sålunda inte vara problematiska med tanke på 1 § i grundlagen.

10.2.10 Tryggande av informationskällor

Den föreslagna reglering om tryggande av en informationskälla i 78 a § i lagförslag 1 i propositionen är relevant med tanke på den straffrättsliga legalitetsprincip som föreskrivits i 8 § i grundlagen. Enligt den får ingen anses vara skyldig till brott och inte heller dömas till straff för en gärning som inte föreskrivits som straffbar genom lag vid gärningstidpunkten. För ett brott får inte ett strängare straff utdömas än vad som föreskrivits genom lag vid gärningstidpunkten. Den straffrättsliga legalitetsprincipen har fått sitt mer konkreta innehåll bland annat i grundlagsutskottets utlåtandepraxis. Den straffrättsliga legalitetsprincipen innehåller ett krav på att regleringen ska vara exakt. Enligt den måste brottsrekvisiten för varje brott uttryckas tillräckligt noggrant i lagen så att man utifrån bestämmelsens lydelse ska kunna förutsäga om en verksamhet eller försummelse är straffbar (GrUU 10/2000 rd, s. 2/I, GrUU 41/2001 rd, s. 2/II, GrUU 48/2002 rd, s. 2). I Europadomstolens och EU-domstolens praxis har legalitetsprincipen i praktiken tilldelats ett motsvarande kärninnehåll, vilket betonar straffregleringen förutsägbarhet, det vill säga att det utifrån bestämmelsens ordalydelse är möjligt att förutse vad som är straffbart (se GrUU 12/2021 rd, s. 14, GrUU 20/2018 rd, s. 2, GrUU 10/2016 rd och GrUU 56/2014 rd, s. 2/II och de utlåtanden till vilka det hänvisats i dessa).

Grundlagsutskottet har i sin vedertagna utlåtandepraxis förutsatt att öppna gärningssätt i straffbestämmelserna i princip är problematiska med tanke på den straffrättsliga legalitetsprincipen (till exempel GrUU 20/2022 rd, s. 4, GrUU 12/2021 rd, stycke 58, GrUU 20/2018 rd, s. 2 och GrUU 6/2014 rd, s. 3/I). Till exempel grundlagsutskottet har i samband med förslaget till ändring av lagen om Forststyrelsens jakt- och fiskeövervakning riktat uppmärksamhet på 19 a § 1 punkten i lagen om Forststyrelsens jakt- och fiskeövervakning, enligt vilken det är straffbart att underlåta att iaktta en order eller ett förbud som en jakt- och fiskeövervakare meddelat inom ramen för sina befogenheter (tredska mot jakt- och fiskeövervakare). Punkten hade en koppling till förslaget om rätten att ge befallning i 4 a § i lagen om Forststyrelsens jakt- och fiskeövervakning, enligt vilken en jakt- och fiskeövervakare som enligt lagen om Forststyrelsens jakt- och fiskeövervakning eller någon annan lag utövar sina befogenheter har rätt att för att genomföra jakt- och fiskeövervakningsuppdraget i enskilda fall ge befallningar och utfärda förbud som är förpliktande för var och en, vilken grundlagsutskottet ansett förbli av jämförelsevis allmän natur. Grundlagsutskottet har ansett att tillämpningsområdet för det straffbara beteendet enligt 19 a § 1 punkten förblir väldigt oklart (GrUU 21/2024 rd, s. 3-4).

Grundlagsutskottet har tagit ställning till användning av begrepp som ansetts ge utrymme för tolkning och vara förenade med bedömning i straffbestämmelser. Till exempel i samband med propositionen om mottagande av muta som riksdagsledamot har grundlagsutskottet konstaterat att olika synpunkter kan läggas fram beträffande exempelvis när en riksdagsledamot förfarit på det sätt som avses i den föreslagna bestämmelsen ”på grund av förmånen” som ska betraktas som muta och att det finns utrymme för tolkning även beträffande när en ledamot i sitt riksdagsuppdrag ska anses ”verka för att ett ärende ... skall bli avgjort på ett visst sätt” (GrUU 29/2001 rd, s. 4). Även till exempel begreppet ”sedvanlig gästfrihet” har ansetts lämna utrymme för bedömning (GrUU 68/2010 rd, s. 5).

I anknytning till en myndighetens prövningsrätt har grundlagsutskottet konstaterat att till exempel bevisprovokation genom köp i utskottets praxis har karakteriserats som en okonventionell befogenhet, som innebär en rätt för polisen att förfara i strid med vissa straffrättsliga förbud utan tjänsteansvar. Utskottet har betonat att sådan tjänsteverksamhet konstitutionellt sett i sig redan är betydande för principen om att förvaltningen ska vara lagenlig. I fråga om bevisprovokation genom köp var det betydelsefullt att man kan anse att principen innebär bland annat att en myndighet utan synnerligen vägande skäl och exakt definierade

förutsättningar inte kan tilldelas nya former av befogenheter att vidta åtgärder, som övrigt är straffrättsligt sanktionerade även om de vidtas av en myndighet (GrUU 5/1999 rd, s. 5). Grundlagsutskottet har konstaterat samma sak även i den färskare revideringen av lagen om militär underrättelseverksamhet från år 2019 (GrUU 36/2018, s. 15).

I det nu behandlade förslaget till bestämmelse har avgränsningen av straffansvaret avgränsat exakt till situationer där informationskällans liv eller hälsa äventyras. Dessutom handlar det om en informationskälla som i enlighet med lagen om militär underrättelseverksamhet kräver att förutsättningarna för personen är uppfyllda, personen registrerar och beslut om att använda en informationskälla fattas. Den krets av personer som omfattas av förslaget till bestämmelse är avgränsad.

Även de beslut som kan fattas av huvudstabens underrättelsechef har avgränsats till att informationskällan ordnas till Finland.

Målen med förslaget till bestämmelse kan anses vara motiverade och man kan anse att man genom ändringarna skyddar ett viktigt rättsobjekt, det vill säga någon annans liv och hälsa.

10.2.11 Andra omständigheter som ska bedömas

Information om sabotageprogram

Grundlagsutskottet har bedömt förhållandet mellan ett sabotageprogram eller ett kommando och 10 § 2 mom. i grundlagen i sin utlåtandep Praxis från den senaste tiden. I sitt utlåtande (GrUU 62/2024 rd, punkt 12) om regeringens proposition om en cybersäkerhetslag (RP 57/2024 rd) riktade grundlagsutskottet uppmärksamhet på att sådana i lagförslagen avsedda meddelanden som innehåller ett skadligt datorprogram eller kommando helt faller utanför tillämpningsområdet för hemligheten i fråga om förtroliga meddelanden i 10 § i grundlagen. Det är alltså inte bara fråga om en sådan omständighet som det hänvisas till i motiveringen till lagstiftningsordningen, det vill säga att ett sådant meddelande inte omfattas av kärnområdet i den rättighet som gäller sekretess i fråga om förtroliga meddelanden. Ett sådant meddelande åtnjuter inte skydd enligt 10 § 2 mom. i grundlagen, och bestämmelser om detta behöver inte bedömas utifrån de särskilda eller de allmänna förutsättningarna för inskränkning av de grundläggande fri- och rättigheterna enligt 10 § 4 mom. (GrUU 62/2024 rd, punkt 12).

I fråga om behandlingen av 18 § 2 mom. i lagförslag 1 i den nu behandlade regeringspropositionen handlar det inte om kommunikation enligt 10 § i grundlagen, varvid bedömningen inte baserar sig på ingripande i de grundläggande fri- och rättigheterna i fråga om utlämnande av uppgifter. Således behöver förslaget till bestämmelse inte bedömas med tanke på 10 § i grundlagen.

Fullgöranderapporten

I lagförslag 6 i propositionen föreslås en ny 41 punkt till 6 § 1 mom. i lagen om Enheten för utredning av grå ekonomi, med stöd av vilken Enheten för utredning av grå ekonomi kan utarbeta en fullgöranderapport till en militärunderrättelsemyndighet för skötseln av dess uppgifter. I den föreslagna bestämmelsen specificeras således på ett noggrant avgränsat sätt den myndighet för vilken det är möjligt att utarbeta en rapport till stöd för dess verksamhet. Enligt den gällande lagen om Enheten för utredning av grå ekonomi kan en fullgöranderapporten utarbetas för skyddspolisen för att skydda den nationella säkerheten mot verksamhet som hotar den. Enligt lagen om Enheten för utredning av grå ekonomi är det möjligt att som

informationskällor till fullgöranderapporterna använda endast sådana uppgifter om den myndighet begär en fullgöranderapport är berättigad att få för det användningsändamål som beskrivits i begäran om utredning. Som en del av Försvarsmakten kan en militärunderrättelsemyndighet få uppgifter enligt 17 § i lagen om Försvarsmakten och personuppgifter enligt lagen om behandling av personuppgifter inom Försvarsmakten.

Förbättring av militärunderrättelsemyndighetens tillgång till information om militära hot och för att skydda den nationella säkerheten anses vara nödvändigt för att Enheten för utredning av grå ekonomi ska kunna utarbeta en fullgöranderapport för militärunderrättelsemyndigheten. Den föreslagna ändringen gäller syftet med militär underrättelseinhämtning enligt 3 § i lagen om militär underrättelseverksamhet.

Grundlagsutskottet har bedömt en rätt att få information som åsidosätter sekretessbestämmelserna genom att fästa uppmärksamhet vid att rätten i sista hand handlar om att den myndighet som är berättigad till uppgifterna i och med de egna behoven åsidosätter de grunder och intressen som skyddas genom den sekretess som gäller den myndighet som innehar uppgifterna. Ju allmänare rätt till information regleringen berättigar till, desto större är faran för att sådana intressen kan åsidosättas väldigt automatiskt. Ju fullständigare en rätt att få information kopplas till de sakliga förutsättningarna i bestämmelserna, desto sannolikare är att man i praktiken behöver motivera en enskild begäran om information.

Vikt har även getts åt att även den som lämnar ut uppgifter i så fall har möjlighet att bedöma begäran om utlämnande med tanke på de lagliga förutsättningarna (GrUU 48/2018 rd). Den som lämnar ut information kan dessutom genom att de facto vägra att uppgifterna lämnas ut ge upphov till en situation där skyldigheten att lämna ut uppgifter, det vill säga tolkningen av bestämmelserna, kan bli föremål för granskning av en extern myndighet. Denna möjlighet är viktig då det gäller att anpassa tillgången till information och sekretessintressena till varandra (se GrUU 17/2016 rd och de utlåtanden till vilka det hänvisats i det).

Förslagens godtagbarhet får stöd av att föremålet för underrättelseinhämtningen är verksamhet som är militär eller som allvarligt hotar den nationella säkerheten och tillgången till informationen är kopplad till syftet med den militära underrättelseinhämtningen och de föremål för militär underrättelseinhämtning som fastställts i underrättelselagarna. Godtagbarheten betonas även av att informationstillgången och grunderna för att lämna ut information är bundna till nödvändighets- eller behövlighetskriterierna.

Användning av informationskällor

Det föreslås att 11 § i lagförslag 1 i propositionen innehåller bestämmelser om att försvarsgrenarna under en militärunderrättelsemyndighets styrning och övervakning har möjlighet till så kallad användning av informationskällor av grundformen.

Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag och lag noggrant iakttas i all offentlig verksamhet. Möjligheten att tillåta inskränkningar av de grundläggande fri- och rättigheterna ska bedömas med tanke på de lagförbehåll som eventuell ingår i de enskilda bestämmelserna om de grundläggande fri- och rättigheterna, men även på de allmänna förutsättningarna för inskränkningar av de grundläggande fri- och rättigheterna (GrUB 25/1994 rd).

Med stöd av 10 § i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Skyddet för privatlivet utgår från att en individ har rätt att leva sitt liv utan att myndigheterna eller andra

utomstående godtyckligt eller på ett obefogat sätt ingriper i hans eller hennes privatliv (GrUU 53/2005 rd, GrUU 13/2005 rd, GrUU 11/2005 rd). Privatlivet omfattar bland annat rätten för en individ att knyta och upprätthålla relationer med andra människor och omgivningen. För att garantera skyddet för privatlivet förutsätts av staten att den avhåller sig från att kränka en individs privatliv. Begreppet ”privatliv” kan förstås som ett allmänt begrepp som gäller en person privata krets. Av hävd skyddas privatlivet genom straffrättsliga metoder (RP 309/1998 rd). Användning av informationskällor är av betydelse med avseende på skyddet för privatlivet, som tryggas i 10 § i grundlagen.

Den i 7 § i grundlagen tryggade rätten till liv samt personlig frihet, integritet och säkerhet är av betydelse för informationskällan själv. Ändringen av polislagen 525/2005 har föreskrivits med grundlagsutskottets medverkan (GrUU 11/ 2005 rd), men grundlagsutskottet behandlade inte användning av informationskällor i sitt utlåtande. Den nya polislagen har föreskrivits med grundlagsutskottets medverkan (GrUU 67/2010 rd). I detta utlåtande behandlade grundlagsutskottet inte heller om användning av informationskällor eller styrd användning av informationskällor.

Användningen av informationskällor är i praktiken avgränsad till uppgifter som försvarsgrenarna fått inom ramen för sina egna uppgifter. Det handlar inte om styrd användning av informationskällor, utan om att personerna på eget initiativ ger egna uppgifter till försvarsgrenarnas tjänstemän. Inget arvode betalas heller för uppgifterna, vilket minskar risken för indirekt styrning av informationskälla genom att ge en belöning om källan ger den önskade informationen.

Försvaret av landet och den nationella säkerheten kan anses vara en godtagbar grund med tanke på systemet med grundläggande fri- och rättigheter för att ingripa i skyddet för privatlivet, vilket skyddats som en grundläggande fri- och rättighet. Med tanke på proportionalitetskravet har användning av informationskällor ett synnerligen tungt samhälleligt intresse i bakgrunden, vilket även är förknippat med målet om att trygga andra personers grundläggande fri- och rättigheter. Begränsningen av skyddet för privatlivet är jämförelsevis liten jämfört med vikten av det samhälleliga intresse som utgör grund för begränsningen. Dessutom har försvarsgrenarnas underrättelseverksamhet inte någon självständig befogenhet till användning av informationskällor, utan den sker under militärunderrättelsemyndighetens styrning och övervakning. Utöver ett vägande samhälleligt behov ska begränsningen av en grundläggande fri- och rättighet vara nödvändig för att uppnå det godtagbara syftet.

10.2.12 Skyddet för personuppgifter

10.2.12.1 Allmänt

Grundlagens 10 § innehåller bestämmelser om skyddet för privatlivet. Enligt paragrafens första moment har var och ens privatliv, heder och hemfrid tryggats. Enligt den andra meningen i momentet föreskrivs skyddet för personuppgifter närmare genom lag. Enligt grundlagsutskottets vedertagna praxis har lagstiftarens handlingsutrymme begränsats både av den här bestämmelsen och av att skyddet för personuppgifter delvis ingår i samma moment som skyddet för privatlivet. Lagstiftaren måste tillgodose denna rätt på ett sätt som är godtagbart med avseende på de grundläggande fri- och rättigheterna överlag (se till exempel GrUU 48/2018 rd, s. 3 och GrUU 13/2016 rd, s. 3–4).

Utskottet har särskilt bedömt att tillåtelse att behandla känsliga uppgifter berör själva kärnan i skyddet för personuppgifter, varför till exempel bildandet av register som innehåller sådana uppgifter bör bedömas i förhållande till villkoren för inskränkningar av de grundläggande fri-

och rättigheterna, i synnerhet med tanke på begränsningarnas acceptabilitet och proportionalitet (se till exempel GrUU 48/2018 rd, s. 3 och de utlåtanden till vilka det hänvisats i det). Även enligt EU:s allmänna dataskyddsförordning ska särskilda kategorier av personuppgifter, som till sin natur är särskilt känsliga med hänsyn till de grundläggande fri- och rättigheterna, åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande fri- och rättigheterna. Utskottet har fäst särskild uppmärksamhet vid att behandlingen av känsliga uppgifter genom exakta och noga avgränsade bestämmelser bör begränsas till det som är absolut nödvändigt (se till exempel GrUU 3/2021 rd, s. 3 och GrUU 14/2018, s. 5).

Grundlagsutskottet har även betonat att skyddet för privatlivet och personuppgifter bör stå i proportion till andra grundläggande och mänskliga rättigheter samt till andra vägande samhälleliga intressen som allmän säkerhet, som i extrema fall kan gå tillbaka på den personliga säkerheten som grundläggande rättighet (GrUU 5/1999 rd, s. 2). Utskottet har ansett att skyddet för privatliv och personuppgifter inte har företräde i förhållande till de andra grundläggande fri- och rättigheterna. Analysen går ut på att samordna och avväga två eller flera bestämmelser om de grundläggande fri- och rättigheterna (se till exempel GrUU 26/2018 rd, s. 4, GrUU 14/2018 rd, s. 8, GrUU 54/2014 rd, s. 2 och GrUU 10/2014 rd, s. 4).

Grundlagsutskottet har inom tillämpningsområdet för EU:s dataskyddsförordning sett över sin ståndpunkt om kravet på att utfärda bestämmelser om skyddet för personuppgifter genom lag. Utskottet anser att dataskyddsförordningens detaljerade bestämmelser, som

tolkas och tillämpas i enlighet med de rättigheter som garanteras i EU:s stadga om de grundläggande rättigheterna, överlag utgör en tillräcklig rättslig grund även med avseende på skyddet för privatlivet och personuppgifter enligt 10 § i grundlagen. Enligt utskottets uppfattning motsvarar regleringen i dataskyddsförordningen, då den tolkas på behörigt sätt, även den nivå på skyddet för personuppgifter vilken fastställs enligt Europakonventionen. Således är det inte längre av konstitutionella skäl nödvändigt att speciallagstiftningen inom dataskyddsförordningens tillämpningsområde heltäckande och detaljerat föreskriver om behandling av personuppgifter (se GrUU 14/2018 rd, s. 4). Grundlagsutskottet har dock sett det som klart att behovet av speciallagstiftning i enlighet med det riskbaserade synsätt som också krävs i dataskyddsförordningen måste bedömas utifrån de hot och risker som behandlingen av personuppgifter orsakar. Ju högre risk som orsakas av behandlingen för en fysisk persons rättigheter och friheter, desto mer motiverat är det med detaljerad reglering. Denna omständighet är av särskild betydelse när det gäller behandling av känsliga uppgifter (se till exempel GrUU 51/2018 rd, s. 3 och GrUU 14/2018 rd, s. 4–6). Grundlagsutskottet har också särskilt lyft fram behovet av reglering i de fall där personuppgifterna behandlas av en myndighet (GrUU 14/2018 rd, s. 4–5).

Grundlagsutskottet har ansett att till skillnad från den direkt tillämpliga dataskyddsförordningen innehåller dataskyddsdirektivet inte några detaljerade bestämmelser som skulle utgöra en tillräcklig rättslig grund för skyddet för privatlivet och personuppgifter i 10 § i grundlagen. Enligt grundlagsutskottet ska regleringen kring behandling av personuppgifter i en sådan regleringskontext som är känslig med avseende på de grundläggande fri- och rättigheterna fortfarande bedömas utifrån utskottets tidigare reglering som betonat bestämmelser på lagnivå, exakthet och omfattning. Kraven på räckvidd för, exakthet hos och noggrann avgränsning av bestämmelser om skyddet för personuppgifter till vissa delar kan dock till viss del uppfyllas genom en allmän nationell lag utanför tillämpningsområdet för dataskyddsförordningen (se GrUU 51/2018 rd, s. 3, GrUU 26/2018 rd, s. 3–4 och GrUU 14/2018 rd, s. 7).

I sin utlåtandepraxis om rättigheterna att få information och utlämnande av uppgifter har grundlagsutskottet fäst uppmärksamhet vid vad och för vem rätten att få uppgifter gäller och hur rätten är kopplad till nödvändighetskriteriet. Det är möjligt att myndigheternas rätt till information och möjlighet att lämna ut information anknutit till uppgifter som är behövliga för ett visst ändamål, om man strävat efter att räkna upp uppgiftsinnehalten på ett uttömmande sätt genom lag. Om innehållet i uppgifterna däremot inte på samma sätt har ansetts i form av en förteckning, ska man enligt utskottet i lagstiftningen ha inkluderat ett krav på att ”informationen är nödvändig” för ett visst syfte. Å andra sidan har utskottet ansett att väldigt rymliga och ospecificerade rättigheter att få uppgifter inte är möjliga med tanke på grundlagen, inte ens om de är förenade med nödvändighetskriteriet. I sina analyser av omfattning, exakthet och innehåll i lagstiftning om rätten att få och lämna ut uppgifter trots sekretess har utskottet lagt vikt vid att de uppgifter som lämnas ut är av känslig art (se till exempel GrUU 48/2018 rd, s. 4–5, GrUU 38/2016 rd, s. 3 och GrUU 17/2016 rd, s. 2–3).

Grundlagsutskottet har ansett att det är viktigt att till den del som EU-lagstiftningen förutsätter eller möjliggör nationell reglering, ska vid användningen av detta nationella handlingsutrymme kraven som följer av de grundläggande och mänskliga rättigheterna beaktas. Utskottet har därför framhållit att det i regeringens propositioner finns anledning att särskilt i fråga om bestämmelser som är av betydelse med hänsyn till de grundläggande fri- och rättigheterna tydligt klargöra ramarna för det nationella handlingsutrymmet (se till exempel GrUU 1/2018 rd, s. 3, GrUU 26/2017 rd, s. 42, GrUU 2/2017 rd, s. 2 och GrUU 44/2016 rd, s. 4).

På behandlingen av personuppgifter vid militärunderrättelsemyndigheten tillämpas beroende på behandlingssyftet antingen lagen om behandling av personuppgifter inom Försvarsmakten (332/2019) eller lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018, nedan dataskyddslagen avseende brottmål). Inom den helhet som dessa lagar bildar tillämpas inte EU:s dataskyddsförordning och inte heller den allmänna dataskyddslagen överhuvudtaget.

Specialregleringen kompletterar den allmänna dataskyddsförordningen (EU 2016/679). Enligt den allmänna dataskyddsförordningen och dataskyddslagen avseende brottmål utgörs personuppgifter av alla sådana uppgifter utifrån vilka en person kan identifieras direkt eller indirekt. Indirekt identifiering kan ske till exempel genom att slå samman en enskild uppgift med en annan uppgift som möjliggör identifieringen. Behandlingen av personuppgifter i militär underrättelseinhämtning omfattas av den allmänna dataskyddsförordningens tillämpningsområdet och baserar sig på artikel 6.1 e, enligt vilken behandling är tillåten för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

I den nu behandlade propositionen föreslås en ny typ av reglering (i synnerhet 66 § och 67 a § i lagförslag 1), där personuppgifter behandlas, men de inte inhämtas för att identifiera en person eller få information om hans eller hennes privatliv. Bestämmelserna handlar framför allt om den tekniska inriktningen av underrättelseinhämtning som avser datatrafik och den tekniska behandlingen av datatrafik som anknyter till fastställandet av närmare sökbegrepp. Genom förslagen är det möjligt att lagra uppgifter som kan användas även i användningen av andra befogenheter och i egentlig underrättelseinhämtning som avser datatrafik.

10.2.12.2 Behandling av tekniska data om datatrafik och fastställande av sökbegrepp

Utgångspunkten i den gällande lagen om behandling av personuppgifter inom Försvarsmakten är att tekniska data om datatrafik, med undantag för styrningstrafiken i anordningarna i datatrafiknätet och annan datatrafik som sker endast mellan anordningar, utgör uppgifter som

direkt eller indirekt anknyter till i identifierbar person, det vill säga personuppgifter. Det motsvarande kan konstateras i fråga om det föreslagna fastställandet av sökbegrepp för underrättelseinhämtning som avser datatrafik.

Även om den föreslagna behandlingen av tekniska data och fastställande av sökbegrepp i regel hänför sig till uppgifter utifrån vilka en person kan identifieras indirekt och förslagen inte ger någon möjlighet att inhämta uppgifter om föremålet för militär underrättelseinhämtning, ger användningen av de uppgifter som inhämtats genom befogenheterna i den egentliga underrättelseinhämtningen som avser datatrafik en möjlighet att kombinera dem med annan information som kan användas eller som används av militärunderrättelsemyndigheten i underrättelseinhämtning som avser datatrafik. Även om behandlingen av tekniska data och fastställande av sökbegrepp innehåller även andra uppgifter än personuppgifter, är det ändamålsenligt att tillämpa förutsättningarna för behandling av personuppgifter på behandlingen av hela informationsmaterialet.

Upptagningar i anknytning till behandling av tekniska data och fastställandet av sökbegrepp enligt propositionen kan omfatta uppgifter som hör till särskilda kategorier av personuppgifter enligt artikel 9 i dataskyddsförordningen eller andra uppgifter som ska anses vara konstitutionellt sett känsliga. I samband med behandling i den egentliga underrättelseinhämtningen som avser datatrafik kan det handla om behandling av ovan nämnda uppgifter. Enligt led g i artikel 9.2 i den allmänna dataskyddsförordningen är behandling av uppgifter som hör till de särskilda kategorierna av persongrupperna möjlig om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträfvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. På ovan beskrivna sätt anses behandlingen även till denna del vara proportionell. Till denna del begränsas behandlingen av de principer som föreskrivs i 3 § i lagen om behandling av personuppgifter inom Försvarsmakten och 11 § i dataskyddslagen avseende brottmål, till vilken det hänvisats i 4 § 2 mom., där lagring av uppgifter som hör till särskilda kategorier av personuppgifter är tillåten endast om behandlingen är nödvändig med tanke på registrets användningsändamål.

10.2.12.3 Jämförelse av personuppgifter

I 37 a § i lagförslag 13 i propositionen föreslås att militärunderrättelsemyndigheten för att administrera sitt informationssystem får jämföra uppgifterna i personregister, varifrån militärunderrättelsemyndigheten kan få uppgifter med stöd av en annan lag, med innehållet i dess lagrade personuppgifter. Uppgifter som inte behövs ska utplånas utan dröjsmål efter att jämförelsen gjorts. Uppgifter som inte behövs får inte lagras.

En militärunderrättelsemyndighet kan redan för närvarande få de uppgifter som avses i bestämmelsen utifrån dess lagstadgade rätt. Således har behandlingen av personuppgifter bedömts i samband med behandlingen av respektive lag. Den jämförelse som bestämmelsen möjliggör kan anses göra att militärunderrättelsemyndighetens personregister är bättre uppdaterade och således kan den anses ha positiva konsekvenser för de grundläggande fri- och rättigheterna.

Den föreslagna bestämmelsen kan inte anses vara särskilt betydelsefull med tanke på integritetsskyddet, eftersom möjliggörandet av jämförelsen inte utvidgar det uppgiftsinnehåll till vilket militärunderrättelsemyndigheten redan för närvarande har rätt. Bestämmelsen förtydligar lagstiftningen och gör den noggrannare avgränsad till den del som

militärunderrättelsemyndigheten genom en teknisk förbindelse eller som ett dataset har rätt att få behövliga personuppgifter för att utföra sina uppdrag och för att administrera sina register. Bestämmelsen ändrar inte på det rådande rättsläget, men beaktar de krav som den tekniska utvecklingen ställer på dataskyddet och registrets korrekthet.

10.2.12.4 Sammandrag

På den praktiska operativa nivån har dataskyddskraven vid Militärunderrättelsemyndigheten beaktats redan i fråga om behandling av tekniska data och egentlig underrättelseinhämtning som avser datatrafik, eftersom det handlar om en befintlig befogenhet och åtgärder som redan varit i kraft. Ändringarna av sakinnehållet i regleringen bedöms inte ha konsekvenser för de valda dataskyddslösningarna. I fråga om fastställandet av sökbegrepp handlar om ett nytt sätt att behandla personuppgifter. Till denna del ska man från första början i det praktiska genomförandet beakta det inbyggda och förvalda dataskyddet samt dataskyddsprincipen. Dataskyddsprinciperna har föreskrivits i 3 § i lagen om behandling av personuppgifter inom Försvarsmakten, vilken omfattar säkerställande av lagenligheten, användningsändamålsbundenheten, minimering av de uppgifter som behandlas, säkerställande av att de uppgifter som behandlas är exakta, begränsning av lagringen av de uppgifter som behandlas och skydd för de personuppgifter som behandlas samt diskrimineringsförbudet. Dataskyddsprinciperna kan anses komplettera de principer som regleras i 5–9 § i lagen om militär underrättelseverksamhet. En Militärunderrättelsemyndighet som fungerar som personuppgiftsansvarig ska vidta alla tekniska och organisatoriska åtgärder för att genomföra dataskyddsprinciperna och skydda de registrerades rättigheter. En Militärunderrättelsemyndighet ska även förvissa sig om att de anordningar, programvaror och andra biprodukter som upphandlas uppfyller de krav som ställts på dem.

I artikel 35 i den allmänna dataskyddsförordningen finns det bestämmelser om skyldigheten att göra en konsekvensbedömning av dataskyddet, om behandling av en viss typ, i synnerhet vid användning av ny teknik, med beaktande av behandlingens art, omfattningar, kontext och ändamål, sannolikt orsakar en hög risk för en fysisk persons rättigheter och friheter. Den föreslagna radiotekniska övervakningen kan omfatta sådana risker. Således ska Gränsbevakningsväsendets stab, som fungerar som personuppgiftsansvarig, innan den nya föreslagna befogenheten införs, genomföra en noggrannare bedömning av konsekvenserna av de planerade behandlingsåtgärderna för skyddet för personuppgifter i enlighet med kraven i den allmänna dataskyddsförordningen. Den personuppgiftsansvarige ska även rikta särskild uppmärksamhet på informationen till dem som rekryteras, eftersom den radiotekniska övervakningen inte meddelas i övrigt enligt den föreslagna regleringen.

Lagen om militär underrättelseverksamhet och lagen om behandling av personuppgifter innehåller omfattande och detaljerade bestämmelser om de personuppgifter som behandlas, innehållet i de uppgifter som behandlas och de tillåtna användningsändamålen, utlämnande och utplånande av personuppgifter samt tillgodoseende av den registrerades rättigheter och undantag från den registrerades rättigheter. I propositionen föreslås inte specialreglering om sådana ärendehelheter som regleras på omfattande och exakt sätt i den allmänna dataskyddslagen. Den allmänna dataskyddsförordningen, dataskyddslagen och dataskyddslagen avseende brottmål innehåller detaljerade bestämmelser bland annat om den personuppgiftsansvariges ansvar de registrerades rättigheter och övervakningen av behandlingen av personuppgifter samt om följder av lagstridig behandling av personuppgifter.

10.3 Lagen om försvarsmakten

10.3.1 Inhämtande av information från allmänt tillgängliga källor

I lagförslag 2 i propositionen föreslås att nya 8 b och 8 c § fogas till lagen om försvarsmakten. Bestämmelserna gäller underrättelseinhämtning från tillgängliga källor i allmänhet, det vill säga de informationsresurser som är tillgängliga för alla allmänt eller mot en avgift.

Användningen av offentlig makt ska basera sig på lag. I all offentlig verksamhet ska lag noggrant iaktas. Det finns bestämmelser om denna rättsstatsprincip och principen om förvaltningens laglydighet, vilken väsentligt anknyter till denna, i 2 § 3 mom. i grundlagen.

Tillämpningen av rättsstatsprincipen förutsätter att den som utövar offentlig makt alltid har en behörighetsgrund som i sista hand återgår på en av riksdagen stiftad lag. En myndighet kan således inte ha behörighet att utöva offentlig makt, om behörigheten saknar uttryckligt stöd i lagen.

Underrättelseinhämtning från allmänt tillgängliga källor handlar inte alltid om behandling av personuppgifter. I typfallet innehåller exempelvis information som inhämtats genom datatekniska metoder från allmänt tillgängliga källor dock personuppgifter som anknyter till en person som identifierats eller kan identifieras på det sätt som avses i artikel 4 i den allmänna dataskyddsförordningen och 3 § i dataskyddsförordningen avseende brottmål. Förslaget är således viktigt i synnerhet med tanke på det i 10 § i grundlagen tryggade skyddet för privatlivet och skyddet för personuppgifter.

I artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna förutsätts att behandlingen av personuppgifter ska ske för ett visst ändamål. Enligt artikel 5.1 b i dataskyddsförordningen ska personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Enligt artikel 5.1 c, som gäller uppgiftsminimering, ska personuppgifterna vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. På motsvarande sätt finns det bestämmelser principen om ändamålsbundenheten och uppgiftsminimering även i artikel 4 i dataskyddsdirektivet för brottmål och nationellt i 5 och 6 § i dataskyddslagen avseende brottmål. Även grundlagsutskottet har i sin bedömning av lagstiftningen om behandling av personuppgifter ansett att bland annat målen registreringen, uppgiftsinnehalten och tillåtna användningsändamål är viktiga regleringsobjekt med tanke på skyddet för personuppgifter (se till exempel GrUU 51/2018 rd, s. 8 och GrUU 14/2018 rd, s. 2). Utskottet har förutsatt att i synnerhet behandlingen av känsliga uppgifter begränsas genom exakta och noggrant avgränsade bestämmelser på lagnivå till endast vad som är nödvändigt (se till exempel GrUU 51/2018 rd, s. 10).

I sitt utlåtande om den gällande lagen om behandling av personuppgifter i polisen har grundlagsutskottet bedömt ett förslag som bland annat gällde behandling av uppgifter som inhämtats i samband med en riskanalys från offentliga källor i situationer där uppgifterna inte direkt gäller en aktuell enskild uppgift för polisen. Den föreslagna bestämmelsen hade möjliggjort att uppgifter lagras i polisens register i sex månader för att bedöma deras betydelse. Enligt grundlagsutskottets uppfattning har regleringen genererat ett omfattande register som i fråga om uppgiftsinnehåll och behandling var juridiskt sett okontrollerbart, vilket även kunde innehålla en stor mängd känsliga uppgifter. Förslagen till bestämmelser hade möjliggjort att uppgifter som är betydelselösa för polisens uppgifter samlas in och lagras i registret i till och med sex månader. (GrUU 51/2018 rd, 9–10.)

Grundlagsutskottet ansåg att en förutsättning för att behandla lagförslaget i vanlig lagstiftningsordning var att bestämmelserna av den föreslagna formen skulle slopas. Utskottet anmärkte dock att det trots grundlagen är möjligt att utfärda bestämmelser om bedömningen av grunderna för behandling av personuppgifter till exempel genom reglering som gäller utplåning av samma typ som reglering som utfärdats med grundlagsutskottets medverkan (GrUU 60/2010 rd, s. 4/ II—5/I) i 5 kap. 55 § i polislagen (se även tvångsmedelslagens 57 § och GrUU 66/2010 rd, s. 10 samt GrUU 32/2013 rd, s. 6—7). (GrUU 51/2018 rd, 9–10.). I 5 kap. i lagen om behandling av personuppgifter inom Försvarsmakten finns det detaljerade bestämmelser om utplåning av uppgifter.

På det i propositionen föreslagna inhämtandet av information från allmänt tillgängliga källor tillämpas lagen om behandling av personuppgifter inom Försvarsmakten, då den inhämtande informationen omfattar personuppgifter. Personuppgifterna ska således utplånas enligt vad som föreskrivs om ett ändamålsbundet register. Därtill innehåller lagens 45 § bestämmelser om att en personuppgift ska raderas från ett tillfälligt personregister direkt efter att den inte längre behövs för användningsändamålet. Behövligheten av ett tillfälligt personregister ska bedömas åtminstone med tre års mellanrum.

Även regleringen i lagen om behandlingen av personuppgifter inom Försvarsmakten blir tillämplig, såsom det nödvändighetskrav som föreskrivits för behandling av personuppgifter som hör till särskilda kategorier av personuppgifter. Utöver personuppgifter ska även uppgifter som inhämtats från allmänt tillgängliga källor enligt föreslagna 8 c § i lagen om försvarsmakten utplånas utan dröjsmål efter att det kommit fram att informationen inte behövs för att sköta Försvarsmaktens uppgifter.

Även om 8 b § i lagförslag 2 i propositionen inte kan anses handla om utövning av offentlig makt, kan verksamheten dock anses vara i den mån central i det moderna samhället att det finns ett behov av att utfärda bestämmelser om den genom lag. I synnerhet den föreslagna användningen av en täckidentitet i 3 mom. i bestämmelsen utgör verksamhet som en myndighet inte kan anses genomföra utan uttrycklig bestämmelse i lag.

10.3.2 Tjänsteutnämningar

I lagförslag 2 i propositionen föreslås att ett nytt 3 mom. fogas till 36 a § i lagen om försvarsmakten.

Enligt 2 § i grundlagen ska all utövning av offentlig makt bygga på lag och lag noggrant iakttas i all offentlig verksamhet. Utövning av offentlig makt alltid ska alltid kunna återgå på en befogenhetsgrund i en av riksdagen stiftad lag (RP 1/1998 rd). Enligt 80 § 1 mom. i grundlagen ska bestämmelser om grunderna för individens rättigheter och skyldigheter utfärdas genom lag.

De föreslagna bestämmelserna är relevanta med hänsyn till grundlagens 6 § som gäller jämlikhet, 7 § som gäller rätten till liv och till personlig frihet, integritet och trygghet, 18 § som gäller rätten till arbete och det allmännas skyldighet att sörja för skyddet av arbetskraften, 12 § som gäller offentlighet och 21 § som gäller rättsskydd. Enligt 22 § i grundlagen ska det allmänna se till att de grundläggande fri- och rättigheterna och de mänskliga rättigheterna tillgodoses. Regleringen kan dessutom granskas med hänsyn till artikel 2.1 i Europeiska konventionen om skydd för de mänskliga rättigheterna (Europakonventionen) som gäller rätten till liv, och artikel 6.1 i konventionen som gäller rätten till en rättvis rättegång. Vidare har grundlagsutskottet i sitt utlåtande om statsrådets redogörelse om de mänskliga rättigheterna 2014 särskilt belyst att beredningen av propositioner bör utvecklas för att lagstiftningsordningen ska motiveras också med avseende på skyldigheten enligt 22 § i grundlagen att se till att de grundläggande fri- och

rättigheterna och de mänskliga rättigheterna tillgodoses och inte enbart med avseende på eventuella motsatsförhållanden i fråga om rättigheterna (GrUU 52/2014 rd, s. 3/II). Artikel 17 i Europakonventionen gäller förbud mot missbruk av rättigheter.

De grundläggande fri- och rättigheterna har inte ställts i inbördes prioritetsordning. Propositionen är förknippad med olika grundläggande fri- och rättigheter och mänskliga rättigheter, och deras inbördes förhållande och samordning måste vägas mot varandra. Vidare bör de mänskliga och grundläggande fri- och rättigheterna granskas med hänsyn till vägande samhälleliga intressen, såsom den nationella säkerheten eller den allmänna säkerheten. Intresset av att trygga den allmänna säkerheten handlar i kontexten grundläggande fri- och rättigheter i extrema fall om att trygga den personliga säkerheten (se GrUU 5/1999 rd, s. 2). Hänsyn bör även tas till de allmänna förutsättningarna för inskränkning i grundläggande fri- och rättigheter, bland annat att inskränkningarna ska vara noga avgränsade och tillräckligt exakt definierade och att deras innehåll till väsentliga delar ska framgå av lagen (GrUB 25/1994 rd, s. 5). Vidare ska grunderna för inskränkningar vara godtagbara och inskränkningarna ska vara dikterade av något tungt vägande samhälleligt skäl. Det kan inte genom vanlig lag föreskrivas om en inskränkning av kärnan i en grundläggande fri- eller rättighet. Inskränkningarna ska vara förenliga med kravet på proportionalitet och nödvändiga för att uppnå ett acceptabelt syfte. Inskränkningar i grundläggande fri- och rättigheter kräver ett adekvat rättsskydd.

I 6 § i grundlagen ingår en allmän jämlikhetsklausul och ett diskrimineringsförbud. Jämlikhetsaspekterna är relevanta på så sätt att människor inte godtyckligt genom lag kan särbehandlas vare sig positivt eller negativt. Jämlikhetsbestämmelsen förutsätter dock inte att alla medborgare ska bemötas likadant i alla avseenden, om inte de förhållanden som inverkar på ärendet är likadana (RP 309/1993 rd, s. 45–48). De krav som ställs på en godtagbar grund som möjliggör särbehandling enligt 6 § 2 mom. i grundlagen har i grundlagsutskottets praxis förutsatts ha ett sakligt och fast samband med lagens syfte (till exempel GrUU 44/2010 rd). Den reglering som nu föreslås kan inte anses vara problematisk med tanke på jämlikhetsprincipen. Tillsättande av vissa uppgifter hos Försvarsmakten utan att offentligt ledigförklara dem försätter i sig inte människor i en olik ställning. Det finns godtagbara och vägande samhälleliga skäl för att tillämpa ett avvikande förfarande för tillsättning av tjänster. Det är dock viktigt att beakta jämlikhetsaspekten som en del av Försvarsmaktens personalpolicy.

I anknytning till 7 § i grundlagen har grundlagsutskottet yttrat sig som det exceptionella hotet mot den personliga säkerheten i anknytning till Försvarsmaktens internationella uppdrag (GrUU 65/2016 rd). Enligt grundlagsutskottet kan internationella uppdrag enligt lagförslaget inbegripa användning av militära maktmedel och således medföra exceptionellt hot mot den personliga säkerheten, vilket är relevant också med avseende på 7 § i grundlagen. År 2020 har grundlagsutskottet i anknytning till de förordningar som utfärdas med stöd av beredskapslagen framfört synvinklar om skyldigheten enligt 7 § 1 mom. för det allmänna att trygga var och ens rätt till liv (GrUB 2/2020 rd). I grundlagsutskottets betänkande GrUB 5/2020 rd har utskottet i samband med behandlingen av statsrådets förordning om temporära undantag vid tillämpningen av vissa bestämmelser i semesterlagen, arbetstidslagen och arbetsavtalslagen, som utfärdats med stöd av beredskapslagen, även ägnat uppmärksamhet åt det allmännas skyldighet enligt 18 § 1 mom. i grundlagen att sörja för skyddet av arbetskraften.

I sin nyaste praxis har grundlagsutskottet bland annat i fråga om lagförslaget om offentligheten för skyddspolisens utnämningsförfarande konstaterat att målen för begränsning av offentligheten har en koppling till 7 § i grundlagen, men även till skyldigheten för det allmänna att skydda arbetskraften enligt 18 § i grundlagen. Utskottet ansåg att det med tanke regleringens godtagbarhet var viktigt att avvikelser från offentligheten för ansökningsförfarandet förutsätter en bedömning som görs från fall till fall.

När det gäller sökande av ändring i beslut om utnämning till en tjänst bör förslaget bedömas med hänsyn till bestämmelsen om rättsskydd i 21 § i grundlagen och artikel 6.1 i Europakonventionen (rätten till en rättvis rättegång). Enligt 21 § 1 mom. i grundlagen har var och en rätt att få ett beslut som gäller hans eller hennes rättigheter och skyldigheter behandlat vid domstol eller något annat oavhängigt rättskipningsorgan. Enligt 21 § 2 mom. i grundlagen ska dessutom rätten att söka ändring på samma sätt som garantierna om en rättvis rättegång och god förvaltning tryggas. Avsikten är dock inte att genom bestämmelsen förhindra att det föreskrivs om mindre undantag från denna rättighet, under förutsättningen att de i enskilda fall riskerar individens rättighet till rättvis rättegång (RP 309/1993 rd, s. 79).

Vid beslut om utnämning till en tjänst ska myndigheten, utöver behörighetskraven och övriga eventuella särskilda krav som gäller den ifrågavarande tjänsten, iakttäta den allmänna grunderna för utnämning till en tjänst som föreskrivs i 125 § 2 mom. i grundlagen. Ingen har dock någon rätt som kan betraktas som subjektiv att bli utnämnd till en statlig tjänst. En ändring av statstjänstemannalagen trädde i kraft vid ingången av 2019. I lagens 59 § föreskrivs det om sökande av ändring i ett beslut om utnämning till en tjänst. I regeringens proposition om ändringen av statstjänstemannalagen (RP 77/2017 rd) har denna fråga bedömts med stöd av grundlagsutskottets utlåtanden (GrUU 63/2010 rd, GrUU 16/2000 rd, GrUU 10/2009 rd, GrUU 46/2002 rd, GrUU 18/2011 rd, GrUU 51/2010 rd). Grundlagsutskottets utlåtande om ovan nämnda regeringsproposition (GrUU 42/2017 rd) redogör för att frågan om förbudet att överklaga statens tjänsteutnämningar har behandlats flera gånger i grundlagsutskottet och att utskottets tidigare ståndpunkt legat till grund för ovan nämnda ändring av statstjänstemannalagen. Enligt grundlagsutskottets utlåtande hindrar inte bestämmelsen i 21 § i grundlagen att man genom lag föreskriver om mindre undantag från de rättigheter som skyddas där, under förutsättning att undantagen inte ändrar den aktuella rättsskyddsgarantins ställning som huvudregel eller äventyrar individens rättssäkerhet (se till exempel GrUU 68/2014 rd, s. 3/I). Grundlagsutskottet konstaterar vidare att vilken som helst myndighetsåtgärd som är gynnsam för den enskilde dock inte är ett i grundlagen avsett beslut som gäller den enskildes rättigheter. Grundlagsutskottet har ansett att utnämning till en tjänst i utskottets praxis inte har betraktats som en subjektiv rätt så att en person skulle ha rätt att få sin sak behandlad av en domstol på det sätt som avses i 21 § i grundlagen och i artikel 6.1 i Europakonventionen. I utnämningsbesluten ingår dock prövning, och prövningsrätten styrs och begränsas genom lagstiftning. Utgångspunkten för prövningen är 125 § 2 mom. i grundlagen, där det föreskrivs om de allmänna utnämningssubjektens för offentliga tjänster.

Utifrån artikel 6 i Europakonventionen är utnämning till en tjänst inte ett beslut som gäller en persons rättigheter eller skyldigheter. Konventionsbestämmelsen kan inte i sig anses hindra att rätten att söka ändring slopas. Huruvida artikel 6.1 i Europakonventionen kan tillämpas på tjänstemannarättsliga ärenden har bedömts i Europadomstolens avgöranden. En central fråga har vid denna tidpunkt varit om det ärende som gäller en tjänsteman är sådant där man beslutar om hans eller hennes rättigheter och skyldigheter och där tillgången till domstol således ska tryggas.

I sitt utlåtande om regeringens årsberättelse år 2015 (GrUU 25/2016 rd—K10/2016 rd) konstaterade grundlagsutskottet att enligt den utredning som den fått var utnämningarna bland annat av republikens president och statsrådets allmänna sammanträde och ett stort antal utnämningsavgöranden inom till exempel försvars- och utrikesförvaltningen förknippade med sådana särdrag som ger skäl till specialarrangemang. Grundlagsutskottet konstaterade i sitt utlåtande att en grundläggande fråga i utredningen är om besvärsmöjligheten kan vara absolut och gälla alla tjänsteförhållanden.

I propositionen föreslås det inte att rätten att söka ändring slopas när en tjänst eller ett tjänsteförhållande tillsätts genom offentlig utlysning. Ett offentligt ansökningsförfarande ska även i fortsättningen vara huvudregeln i förfarandet för tillsättning av tjänster.

Enligt 12 § 2 mom. i grundlagen är handlingar och upptagningar som innehas av myndigheterna offentliga, om inte offentligheten av tvingande skäl särskilt har begränsats genom lag. Var och en har rätt att ta del av offentliga handlingar och upptagningar. I propositionen föreslås det att det i det offentliga ansökningsförfarandet blir möjligt att begränsa offentligheten för en identifieringsuppgift om en person, det vill säga att lämna ut namnet, i ett meddelande om tillsättandet av en tjänst, vilket vid sidan om övriga grunder är förknippat med ett synnerligen viktigt allmänt intresse, såsom skyddet av den nationella säkerheten och ett skyddet av ett synnerligen viktigt privat intresse, i extrema fall liv och hälsa. Den föreslagna bestämmelsen har inte formulerats som en sekretessbestämmelse. I 12 § 2 mom. i grundlagen möjliggör även andra typer av begränsningar av offentligheten (GrUU 8/2021 rd, s. 8). Sekretessbeläggningen av namnet och annan information ska bedömas utifrån 24 § i offentlighetslagen vid en begäran om information (den allmänna offentligheten) och i fråga om partsoffentligheten utifrån 11 § 1 mom. och 2 mom. 1 punkten i offentlighetslagen. I den föreslagna regleringen bestäms det intresse som ska skyddas i enlighet med bestämmelserna om sekretess i offentlighetslagen, och förslaget ger en ram för ett förfarande med en mer begränsad öppenhet.

Att tjänster och tjänsteförhållanden tillsätts utan ett öppet ansökningsförfarande avviker från den principiella öppenheten och offentlighetsprincipen inom förvaltningen. I enlighet med de allmänna förutsättningarna för inskränkning av de grundläggande fri- och rättigheterna föreslås det att bestämmelser om inskränkningen utfärdas genom lag. Undantaget motiveras emellertid av ett godtagbart och tungt vägande samhälleligt intresse och det har begränsats till vad som är nödvändigt. Undantaget står således i rätt proportion till begränsningen och dess syfte. Det är inte möjligt att utarbeta någon uttömmande förteckning över Försvarsmaktens tjänster med uppgifter som förutsätter att tjänsten tillsätts utan ansökningsförfarande, och Försvarsmakten ska kunna visa att det med tanke på den ifrågavarande uppgiften i varje enskilda fall är nödvändigt att tillsätta tjänsten utan offentlig ansökan. Den exakta och noggranna avgränsningen sker via Försvarsmaktens utnämningsbehörighet, med beaktande av de föreskrivna grunderna för bedömning av nödvändigheten. Enligt förslaget ska det för avvikelse från det allmänna offentliga ansökningsförfarandet finnas en objektiv grund som avser den nationella säkerheten och statens intresse, med beaktande även av att ingen har en subjektiv rätt att bli utnämnd. Det rör sig om en personkrets som begränsas utifrån arbetsuppgifterna, och den föreslagna regleringen innebär ett begränsat och godtagbart undantag. Vissa tjänster på chefsnivå eller motsvarande uppgifter ska enligt förslaget alltid tillsättas i ett offentligt ansökningsförfarande.

Enligt artikel 2 i Europakonventionen ska envars rätt till liv skyddas genom lag. Rätten till liv är den mest centrala grundläggande fri- och rättigheten, och livsfara är det allvarligaste hotet med tanke på enskilda tjänstemän. Lagförslaget gäller ett vägande samhälleligt intresse, landets försvar och den nationella säkerheten. För Finlands landsförsvar och avvärjandet av hot mot den nationella säkerheten och för att förebygga sådana är det nödvändigt för Försvarsmakten att förmå att agera med metoder där hälsan och livet för dem som utför uppdrag i anknytning till dessa kan skyddas från första början. I brottsbekämpningen och militär underrättelseinhämtning är personkretsen även bredare och den täcker även skydd av utomstående, såsom informationskällor. De ovannämnda hoten riktar sig mer allmänt även mot samhället och dess medlemmar och inte i första hand mot individen. Då handlar det i vidare bemärkelse om att skydda samhällsmedlemmarnas grundläggande och mänskliga rättigheter, av vilka de mest betydelsefulla är rätten till liv. De metoder som föreslås i propositionen baserar sig på lag och kan anses vara proportionerliga för att uppnå ett godtagbart mål.

10.4 Exakthet, noggrann avgränsning och proportionalitet i fråga om inskränkningar av de grundläggande fri- och rättigheterna

Nödvändighet

Enligt 10 § 4 mom. i grundlagen är nödvändighet en förutsättning för att begränsa skyddet av hemligheten i fråga om förtroliga meddelanden. Denna förutsättning följer också av de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna.

Vid bedömningen av nödvändigheten av bestämmelserna i lagförslagen ska man beakta att man genom en metod för underrättelseinhämtning som innebär en inskränkning av skyddet för hemligheten för förtroliga meddelanden kan inhämta information endast om sådan verksamhet som är föremål för militär underrättelseinhämtning (4 § i lagen om militär underrättelseverksamhet), som är av militär natur eller som allvarligt hotar den nationella säkerheten. Objektet för militär underrättelseverksamhet har fastställts på uttömmande sätt i lagen, vilket motsvarar kraven i Europadomstolens avgörandepraxis. Till exempel enbart ett omnämnande i lag om att hemliga befogenheter får användas för att skydda den nationella säkerheten är inte tillräckligt för att fullgöra kravet på förutsägbarhet (Zakharov mot Ryssland). Å andra sidan kan en nationell lag inte förutsättas innehålla någon exakt och uttömmande förteckning över de situationer där myndigheterna får använda hemliga befogenheter. En bestämmelse i lag om att terrorhot är en grund för utövande av hemliga befogenheter kan till exempel anses uppfylla det krav på förutsebarhet som ställs i Europakonventionen (Szabó & Vissy mot Ungern).

I 4 § i lagen om militär underrättelseverksamhet, vilken gäller objekten för militär underrättelseinhämtning specificeras och konkretiseras den reglering som ingår i 10 § 4 mom. i grundlagen, enligt vilken man med verksamhet som allvarligt hotar den nationella säkerheten, utöver militär underrättelseinhämtning, avser verksamhet som hotar den demokratiska stats- och samhällsordningen, grundläggande samhällsfunktioner, ett stort antal människors liv eller hälsa eller internationell fred och säkerhet. Eftersom varje punkt i den först nämnda bestämmelsen kan härledas ur ett eller flera skyddsintressen som täcks av begreppen militär verksamhet eller den nationella säkerheten, har paragrafen till denna del uppfyllt de accentuerade kraven på nödvändighet och förutsägbarhet.

I den aktuella propositionen föreslås nya befogenheter, som hänför sig till ovan nämnda objekt för militär underrättelseverksamhet. Eftersom statlig verksamhet, som framför allt utgör objekt, har stora resurser och aktörernas förfaringssätt utvecklas i tilltagande takt, ska militärunderrättelsemyndigheten kunna inhämta behövlig information även utanför det egentliga innehållet i ett meddelande för att kunna rikta befogenheterna på ett behörigt sätt.

Genom den föreslagna regleringen skyddas framför allt andra grundläggande fri- och rättigheter och det finns ett vägande samhälleligt intresse för regleringen.

Exakthet och noggrann avgränsning

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 utövning av offentlig makt bygga på lag och i all offentlig verksamhet ska lag noggrant iaktas. 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. 75/II). För lagar gäller det allmänna kravet på att en lag ska vara exakt och noga avgränsad. Enligt utskottets uppfattning är reglering kring befogenheter

i allmänhet betydelsefull även med tanke på de grundlagstryggade grundläggande fri- och rättigheterna (se GrUU 67/2016 rd, GrUU 10/2016 rd).

De allmänna förutsättningarna för användning av metoderna för underrättelseinhämtning har sammanställts till 12 § i lagen om militär underrättelseverksamhet (Aman mot Schweiz, Kopp mot Tyskland, Kruslin mot Frankrike, Huvig mot Frankrike). Den allmänna förutsättningen för alla metoder för underrättelseinhämtning är att användningen av metoden för underrättelseinhämtning är nödvändig och att det genom den på befogade grunder är möjligt att anta att den ger viktig information för underrättelseuppdraget. Om en metod för underrättelseinhämtning riktas mot en statlig aktör, är en allmän förutsättning för användningen av metoden att informationen behövs för ett underrättelseuppdrag. Det handlar om det så kallade förväntade resultatet.

Eftersom fastställandet av sökbegrepp och annan underrättelseinhämtning än underrättelseinhämtning som hänför sig till någon annan än en statlig aktör kan innehålla avsevärda inskränkningar i fråga om en privatpersons skyddade rättsobjekt, är nödvändighet en förutsättning för användning av dessa metoder. En särskild förutsättning för underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer är därtill att uppgifterna inte kan inhämtas med en annan metod för underrättelseinhämtning.

Det föreskrivs också om särskilda förutsättningar för användningen av metoderna för underrättelseinhämtning och det föreskrivs om dessa förutsättningar i samband med var och en av metoderna i fråga (Aman mot Schweiz, Kopp mot Tyskland, Kruslin mot Frankrike, Huvig mot Frankrike). Regleringen kring befogenheterna redogör för vad som får göras då befogenheterna utövas och hur man då ska förfara, uppgiftsinnehållet i ett yrkande och ett beslut, vilken aktör som beslutar om underrättelseinhämtning, tillståndet för underrättelseinhämtningen, giltighetstiden för ett beslut eller ett yrkande, eventuella förbud mot avlyssning, observation, kopiering och underrättelseinhämtning, på samma sätt som underrättelse om användning av underrättelseinhämtning eller avstående från underrättelse om sådan. Bestämmelserna i anknytning till rättsskyddet är tydliga.

Godtagbarhet och proportionalitet

Vid militär underrättelseinhämtning ska man enligt lagen respektera de grundläggande fri- och rättigheterna och iaktta proportionalitetsprincipen, principen om minsta olägenhet, principen om ändamålsbundenhet och diskrimineringsförbudet. Principerna styr all underrättelseverksamhet.

Bland de motiverade metoderna för underrättelseinhämtning ska en myndighet för militär underrättelseverksamhet, då den utövar befogenheter för underrättelseverksamhet, välja den som bäst främjar att de grundläggande fri- och rättigheterna och de mänskliga rättigheterna tillgodoses.

Proportionalitetsprincipen förutsätter att man gör en bedömning av om användningen av en metod för underrättelseinhämtning kan försvaras i förhållande till vikten av det uppdrag som gäller underrättelseinhämtning, dess brådska, det eftersträfvade målen andra omständigheter som påverkar helhetsbedömningen av situationen. Europadomstolen och EU-domstolen har sin avgörandepraxis betonat vikten av att iaktta proportionalitetsprincipen i synnerhet i samband med underrättelseinhämtning som avser datatrafik (till exempel Zakharov mot Ryssland, Weber och Saravia mot Tyskland, Digital Rights Ireland). Därför förutsätts att underrättelseinhämtning som avser datatrafik och fastställande av sökbegrepp är den sista metod som kan tillgripas, det vill säga att det med en annan metod är omöjligt eller orimligt svårt att inhämta informationen.

Dessutom förutsätts att fastställandet av sökbegrepp är nödvändigt. Dessutom förutsätter underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer att uppgifterna inte kan inhämtas på annat sätt.

Principen om minsta olägenhet leder till att man med militärunderrättelsemyndighetens åtgärder 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 underrättelseuppdraget.

En militärunderrättelsemyndighet får i enlighet med principen om ändamålsbundenhet utöva sina underrättelsebefogenheter endast för ett föreskrivet syfte.

Åtgärderna inom militär underrättelseinhämtning ska riktas utan diskriminering. En uttrycklig bestämmelse om detta har införts i lagen om militär underrättelseverksamhet. Inriktningen av en åtgärd inom den militära underrättelseinhämtningen får inte utan godtagbart skäl grunda sig på en persons ålder, kön, ursprung, nationalitet, bosättningsort, språk, religion, övertygelse, åsikt, politiska verksamhet, fackföreningsverksamhet, familjeförhållanden, hälsotillstånd, funktionsnedsättning, sexuella läggning eller någon annan orsak som gäller hans eller hennes person. Regleringen stärker principen om jämlikhet enligt 6 § 2 mom. i grundlagen i underrättelseverksamhet.

Rättsskyddsarrangemangen

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.

En underrättelsemyndighet kan ha obegränsad prövningsrätt för att rikta underrättelseinhämtning. Ett sätt att begränsa myndighetens prövningsrätt är att tilldela beslutsfattandet om användning av metoder för underrättelseinhämtning som orsakar det allvarligaste ingreppet i skyddet för de grundläggande fri- och rättigheterna till en domstol (bland annat Weber och Saravia mot Tyskland). Underrättelsemyndigheten kan inte heller ha direkt och obegränsat tillträde till datatrafiknäten (Kennedy mot Förenade kungariket). Detta förebyggs genom förutsättningar och principerna för användning av en metod för underrättelseinhämtning, men därtill genom att genomförandet av en koppling mellan exempelvis teleavlyssning och underrättelseinhämtning som avser datatrafik sköts av en instans utanför myndigheten.

Enligt Europadomstolen ska området för tillståndsprövningen framgå av lag. Enligt förslaget ska yrkandets och beslutets innehåll regleras genom lag. 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. Tillståndets längd regleras även på ett noggrant avgränsat sätt.

10.5 Förslagen till bestämmelser i förhållande till Europadomstolens avgörandepraxis

10.5.1 Underrättelseinhämtning som avser datatrafik

Europadomstolen har i ett stort antal avgöranden konstaterat att underrättelseinhämtning som avser datatrafik är möjligt med stöd av artikel 8 i Europakonventionen och att den omfattas av den nationella prövningsrätten. Europadomstolen har även konstaterat att den nationella

prövningsrätten i fråga om omfattningen av den nationella säkerheten och de metoder som ska användas hör till medlemsstaterna inom området för nationell säkerhet.

I sin nyaste avgörandepraxis om underrättelseinhämtning som avser datatrafik har Europadomstolen upprepat sin långvariga linje om underrättelseinhämtning som avser datatrafik, men även utvecklat sin avgörandepraxis om de förutsättningar som den ställer för tillåten underrättelseinhämtning som avser datatrafik. Så som tidigare konstaterats i avsnitt 5.2.1 om Europadomstolens avgörandepraxis, finns det numera åtta, i stället för tidigare sex, förutsättningar för godtagbarhet.

Det bör även observeras att underrättelseinhämtning som avser datatrafik inte har delats in i olika befogenheter, så som i Finland, i Europadomstolens behandling. Således har det med stöd av samma befogenhet varit möjligt att bland annat bevaka den tekniska utvecklingen i datatrafiken, fastställa nya sökbegrepp och inhämta information om det egentliga hotet. Det är illustrerande att Europadomstolen i målet beträffande Centrum för Rättvisa konstaterar att det är en självklarhet att signalspaning utvecklas på det tekniska planet (punkt 207). I den svenska lagstiftningen om signalspaning har det motsvarande konstaterats om fastställande av sökbegrepp endast i motiveringarna till lagen.

Europadomstolen förhåller sig inte absolut negativt till användning av så kallad massaövervakning (bulk interception regime). Europadomstolen anser att allvaret i de hot som avvärjs med den, förmågan hos personerna bakom hoten att agera utan att avslöjas i datanät och oförutsägbarheten för hur den elektroniska kommunikationen dirigeras motiverar att införandet av massaövervakning som har som mål att identifiera hot som äventyrar den nationella säkerheten hör till den nationella prövningssmarginalen. Europadomstolen har även mer generellt ansett att prövningssmarginalen är bred i valet av utbudet av metoder för att trygga den nationella säkerheten (bland annat Weber och Saravia, punkt 106, Big Brother Watch, punkt 274 och Centrum för Rättvisa, punkt 252). Europadomstolen betonar dock att regleringen kring såväl riktade övervakningssystem som massaövervakningssystem i syfte att förhindra maktmissbruk ska uppfylla åtminstone ovan uppräknade minimikrav.

Bestämmelserna i 66 §, 67 §, 67 a §, 67 b §, 68 § och 69 § i lagförslag 1 i den nu behandlade propositionen ska bedömas via de åtta förutsättningar som konstaterats i Europadomstolens nyaste avgörandepraxis. Genom lag ska man utfärda bestämmelser om: 1) grunderna för att tillåta inhämtande av information, 2) de förhållanden där inhämtandet av information kan hänföra sig till en persons kommunikation, 3) förfarandet för att bevilja tillstånd, 4) de förfaranden som ska iakttas i valet, undersökningen och användningen av information, 5) de försiktighetsåtgärder som ska iakttas vid utlämnade av material till olika parter, 6) längden på en åtgärd, begränsningar av lagring av information och de förhållanden då information ska raderas och förstöras, 7) förfaranden och detaljerade bestämmelser med vilka den oberoende myndigheten övervakar att ovan nämnda garantier iakttas och befogenheten för övervakaren att ingripa i lagstridig verksamhet samt 8) oberoende övervakning i efterskott och påföljder.

De bestämmelser till vilka det hänvisats ovan i lagförslag 1 i propositionen är avsevärt mer detaljerade än vad Europadomstolen förutsatt i sin avgörandepraxis. Så som Europadomstolen för fram till exempel i målet beträffande Centrum för Rättvisa, kan underrättelseinhämtning i massaform befinna sig inom den nationella prövningssmarginalen, så länge som förutsättningarna är uppfyllda. I den nu aktuella propositionen har befogenheterna föreskrivits detaljerat och enligt användningsändamålet. Dessutom har användningen av varje befogenhet avgränsats till en viss del av ett kommunikationsnät som överskrider Finlands gräns och därtill till de uppgifter man vill skaffa genom att utöva den ifrågavarande befogenheten, i sista hand utifrån sökbegrepp i den egentliga underrättelseinhämtning som avser datatrafik.

Bestämmelserna omfattar även kvantitativa begränsningar till den del som det inte handlar om så kallad egentlig underrättelseinhämtning som avser datatrafik.

Generellt kan det konstateras att 4 § i lagen om militär underrättelseverksamhet innehåller bestämmelser om de objekt utifrån vilka underrättelseinhämtning som avser datatrafik kan användas och i fråga om metoderna för underrättelseinhämtning har man i bestämmelserna beskrivit mot vad metoden kan riktas. I den helhet som underrättelseinhämtningen utgör har man separat utfärdat processuella bestämmelser om de grunder som ska vara uppfyllda, innan en metod kan användas för att inhämta information. Lagen innehåller även bestämmelser om de förhållanden där underrättelseinhämtning kan hänför sig till en persons kommunikation.

En oberoende domstol beviljar tillstånd till alla befogenheter inom den helhet som underrättelseinhämtning som avser datatrafik bildar. I ett domstolsbeslut fastställs även åtgärdens längd, som är högst sex månader.

Det finns detaljerade bestämmelser om utplåning av information i 82 § och 84 § i lagen och närmare i fråga om egentlig underrättelseinhämtning som avser datatrafik i 86 § i lagen.

Den primära laglighetsövervakningen av verksamheten sker i enlighet med Europadomstolens etablerade avgörandepraxis hos myndigheten själv, det vill säga hos militärunderrättelsemyndigheten. Därtill övervakas verksamheten av Försvarsmaktens assessor och försvarsministeriet.

Det finns bestämmelser om extern övervakning i lagen om övervakning av underrättelseverksamheten. I enlighet med lagen övervakar underrättelsetillsynsombudsmannen militär underrättelseinhämtning i förväg, i realtid och i efterskott. Dessutom kan underrättelsetillsynsombudsmannen avbryta användningen av en metod för underrättelseinhämtning om han eller hon anser att den som är föremål för tillsyn agerat i strid med lag. Underrättelsetillsynsombudsmannen kan även förordna att uppgifterna ska utplånas utan dröjsmål och anmäla ett lagstridigt förfarande som han eller hon observerat för förundersökning.

Dessutom utförs tillsyn av riksdagens justitieombudsman och parlamentarisk övervakning av riksdagens underrättelsetillsynsutskott.

10.5.2 Behandling av tekniska data och fastställande av sökbegrepp

I målet beträffande Centrum för Rättvisa ansåg Europadomstolen även att den i den svenska lagen föreskrivna möjligheten att samla in datatrafik för att utveckla signalspaningen befinner sig inom den nationella provningsmarginalen (punkterna 291–293 i beslutet). I Europadomstolens avgörandepraxis har inte något system av samma karaktär som underrättelseinhämtning som avser datatrafik delats in enligt olika användningsändamål, utan systemet täcker i sin helhet vad som föreskrivs enligt 66 §, 67 a §, 68 § och 70 § i nu föreslagna lagförslag 1. I fallen har man därtill inte tagit ställning till om verksamheten ska vara tillfällig eller dylik.

Det föreslås att 66 § i lagförslag 1 i den nu aktuella propositionen ändras så att den tillfälliga karaktären stryks från den. Dessutom kan befogenheten till att behandla tekniska data användas för att identifiera en i lagen fastställd del av ett kommunikationsnät och därtill för att identifiera dirigeringen av och ändringarna i datatrafiken. Användningen av befogenheten hänför sig endast till tekniska data om datatrafiken.

Enligt förslaget innehåller 66 § i lagförslag 1 i propositionen bestämmelser om grunderna för när underrättelseinhämtning kan tillåtas. Grunderna utgörs av 1) att en statistisk analys görs för att rikta underrättelseinhämtning som avser datatrafik mot en del av ett kommunikationsnät och 2) att dirigeringen av och ändringar i datatrafiken följs. Förslaget till bestämmelse hänför sig inte till en persons kommunikation, eftersom bestämmelse gäller endast för tekniska data om datatrafiken.

Förfarandet för att bevilja tillstånd regleras i 67 § i lagförslag 1. De förfaranden som ska iakttas i valet, undersökningen och användningen av information föreskrivs i 66 § i lagförslag 1, enligt vilken befogenheten gäller tekniska data om datatrafiken, vilka kan användas för de ändamål som nämns i bestämmelsen. I enlighet med vad som föreslås i 67 § gäller ett tillstånd i högst sex månader.

Tekniska data om datatrafik kan även användas i 18 månader efter att de inhämtats i behandlingen av tekniska data och i tolv månader för fastställande av sökbegrepp (67 a § i lagförslag 1) samt i egentlig underrättelseinhämtning som avser datatrafik (68 och 70 § i lagförslag 1). Till övriga delar ska uppgifterna utplånas i enlighet med de förfaranden som föreskrivs i lagen.

Europadomstolen har inte direkt tagit ställning till fastställande av sökbegrepp inom underrättelseinhämtning som avser datatrafik. I målet beträffande Centrum för Rättvis konstaterar Europadomstolen att den i den svenska lagen föreskrivna möjligheten att samla in datatrafik för att utveckla signalspaningen befinner sig inom den nationella prövningsmarginalen (punkterna 291–293 i beslutet). Europadomstolen ansåg inte att det fanns hinder för att datatrafik får samlas in även för utvecklingssyften.

I Europadomstolens avgörandepraxis kan man inte urskilja fall där ett system av samma karaktär som underrättelseinhämtning som avser datatrafik har delats upp på lika detaljerat sätt som i nuläget i Finland och i och med de nu föreslagna ändringarna. Således kan man anses att det finländska systemet är exceptionellt vad gäller exakthet och noggrann avgränsning. Med tanke på Europakonventionen är det därtill relevant även att en domstol fattar ett beslut om befogenheten för varje helhet av underrättelseinhämtning som avser datatrafik.

Således kan det anses att 66 § och 67 a § i lagförslag 1 är problemfria med tanke på Europakonventionen.

10.5.3 Sökbegrepp som gäller innehållet i kommunikationen

I och med de ändringar föreslås för 68 och 70 § i lagförslag 1 i propositionen stryks från bestämmelserna förbudet att använda uppgifter som specificerar terminalutrustning eller en teleadress som innehas eller som i övrigt förmodas användas av en person som vistas i Finland.

Europadomstolen har i sin avgörandepraxis betonat att inhämtande av information ska riktas på datatrafik som överskrider en stats gräns (till exempel Centrum för Rättvisa, punkt 236 och målen Weber och Saravia samt Liberty m.fl. till vilka det hänvisats i det). Detta kan genomföras bland annat genom att hänföra underrättelseinhämtningen till vissa punkter som överskrider statsgränsen och filtrera statens interna datatrafik från mängden. Det har varit möjligt att radera inhemsk datatrafik även i efterskott efter att detta kommit fram, även om det inte heller kan anses vara optimalt.

Europadomstolen har inte tagits ställning till om den andra parten i kommunikationen finnas i hemlandet för den myndighet som använder en metod för underrättelseinhämtning. I de fall som

Europadomstolen behandlat betonas att det handlar om ett gränsöverskridande hot och att det inte finns skäl att rikta så långt gående underrättelseinhämtning mot statens interna datatrafik.

Så som redan förts fram har Europadomstolen ansett att en förutsättning vid bedömning av system av samma natur som underrättelseinhämtning som avser datatrafik är att den baserar sig på användningen av sökbegrepp. Europadomstolen har även godkänt att datatrafik används för att utveckla och rikta systemet. Med andra ord gör Europadomstolen inte någon skillnad mellan om sökbegreppen hänför sig till förmedlingsuppgifterna om kommunikationen eller meddelandets semantiska innehåll – man har inte riktat uppmärksamhet på mot vilka uppgifter och vilken del av datatrafikflödet sökbegreppet riktar sig.

Generellt betonas i Europadomstolens avgörandepraxis att en extern domstol eller ett motsvarande organ ska godkänna de sökbegrepp som används innan användningen av en metod för underrättelseinhämtning börjar.

Det kan inte anses föreligga någon intressekonflikt mellan 68 och 70 § i lagförslag 1 i propositionen och Europakonventionen.

10.5.4 Avstående av underrättelse av underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer

Europadomstolen har i ett stort antal avgöranden, senast beträffande målen Centrum för Rättvisa och Big Brother Watch, tagit ställning till att det med tanke på artikel 8 och artikel 13 i Europakonventionen är centralt om den som blivit objekt för metoder för underrättelseinhämtning har möjlighet att få information om att han eller hon blivit ett objekt. Hur den som blivit objekt eller misstänker att han eller hon blivit objekt får information om ärendet kan genomföras antingen genom en underrättelse eller genom att ett externt oberoende organ ger information om det. I målen Centrum för Rättvisa och Big Brother Watch konstaterar Europadomstolen att personen kan få bättre skydd mot myndigheternas verksamhet från ett organ, till vilket vem som helst med en misstanke om att han eller hon blivit objekt för användning av en metod för underrättelseinhämtning kan överföra sin sak för prövning. I så fall understryks organets självständighet i fråga om underrättelsemyndighetens verksamhet och tillräckliga befogenheter att de facto ingripa i en myndighets verksamhet.

I de system där rättsskyddet baserar sig på underrättelse är det i praktiken möjligt att en person som blivit objekt på grund av olika undantagsarrangemang i praktiken aldrig kan få information om att han eller hon blivit objekt för en metod för underrättelseinhämtning.

I den nu behandlade regeringspropositionen föreslås att underrättelseinhämtning som avser datatrafik inte underrättas till den blivit föremål för sådan. I nuläget ges en underrättelse inte i någon situation till en statlig aktör. Med tanke på Europakonventionen iakttar lösningen den allmänneuropeiska linjen, i praktiken görs inte i något land någon underrättelse om underrättelseinhämtning som avser datatrafik, även om en lagändringsprocess pågår i Sverige i fråga om denna fråga.

I Europakonventionens system kan underrättelseskyldigheten ersättas med andra arrangemang, som garanterar ett motsvarande slutresultat för den som blivit objekt eller som till och med misstänker att han eller hon blivit objekt för användning av en metod för underrättelseinhämtning. På det sätt som konstaterats i Europadomstolens praxis får en person som blivit objekt på detta sätt ofta sin sak behandlad på bättre sätt än utifrån en underrättelse. I den helhet som den finländska underrättelselagstiftningen bildar innebär detta arrangemang underrättelsetillsynsombudsmannens arbete. I helheten ska man därtill beakta att en oberoende

domstol fattar beslut om användning av de metoder för underrättelseinhämtning vilka gör de djupaste inträngen i de grundläggande fri- och rättigheterna.

I fallet Centrum för Rättvis har man tagit ställning till om den svenska myndigheten för övervakning av signalspaning ska ses som ett effektivt rättsmedel. I fallet konstateras att tillsynsmyndigheten ska vara oberoende av underrättelseverksamheten, att övervakaren ska kunna ge juridiskt bindande beslut visavi underrättelsemyndigheten och att den ska övervaka verksamheten i förväg, realtid och i efterskott.

I Finland har underrättelsetillsynsombudsmannen den motsvarande rollen. Ombudsmannens laglighetsövervakning innebär en övergripande laglighetsövervakning av underrättelseverksamheten i förväg (rätten att delta i bland annat domstolsbehandling) i realtid och i efterskott. Ombudsmannen kan förordna att användningen av en metod för underrättelseinhämtning ska avbrytas eller avslutas och i enlighet med lagstiftningen om underrättelsemyndigheter ska de upptagningar och anteckningar som fåtts genom användningen av en metod för underrättelseinhämtning utplånas. Ett beslut om avbrytande eller avslutande av användningen av en metod för underrättelseinhämtning ska hänskjutas till en domstol. Underrättelsetillsynsombudsmannens beslut är rättsligt bindande.

Underrättelsetillsynsombudsmannen kan även ge en anmärkning och bland annat delge tillsynsobjektet sin uppfattning om det lagenliga förfarandet. Till denna del kan det konstateras att militärunderrättelsemyndigheten har iakttagit och implementerat ombudsmannens juridiskt icke-bindande anmärkningar i sin verksamhet.

Vem som helst kan även göra en begäran om undersökning eller framföra klagomål till ombudsmannen.

Enbart år 2024 har ombudsmannen gjort 153 inspektionsbesök hos underrättelsemyndigheterna (jämför med Centrum för Rättvisa punkt 351) och därtill sådana inspektionsbesök som gällde protokoll över användning av metoder för underrättelseinhämtning samt introduktionsbesök som mer allmänt gällde skyddspolisens och militärunderrättelsemyndigheternas verksamhet (underrättelsetillsynsombudsmannens berättelse från år 2024).

Således kan det anses att underrättelsetillsynsombudsmannen uppfyller Europadomstolens krav på garantier för effektivt rättsskydd även i en situation där den som blivit föremål för en metod inte får något meddelande om detta.

10.6 Förslagen till bestämmelser med tanke på EU-domstolens avgörandepaxis

Så som konstaterats tidigare i avsnitt 5.2.2, har Europeiska unionen och dess domstol i sig inte befogenheter att avgöra frågor som gäller medlemsstaternas landsförsvar och den nationella säkerheten. Befogenheten kan dock även vara indirekt, såsom i en situation där en tjänsteleverantör åläggs att lagra och överföra uppgifter som gäller egna kunder och omfattas av integritetsskyddet för behov som hänför sig till landets försvar eller skyddet av den nationella säkerheten.

EU-domstolen har bland annat i sitt avgörande i målet La Quadrature du Net m.fl. mot Premier ministre m.fl. (de förenade målen C-511/18, C-512/18 och C-520/18, punkt 103) ansett att när medlemsstaterna genomför åtgärder som innebär undantag från konfidentialiteten vid elektronisk kommunikation, genom att ålägga tjänsteleverantörer av sådan kommunikation skyldigheter att behandla uppgifter, omfattas skyddet av de berörda personernas uppgifter inte av direktivet om integritet och elektronisk kommunikation. I den föreslagna regleringen ställs

inte skyldigheter för serviceleverantörer inom kommunikation, varför det inte finns något behov av att bedöma regleringen mer ingående ur det nämnda direktivets synvinkel.

Det kan dock konstateras att de här behandlade förslagen till bestämmelser ligger i linje med Europeiska unionens stadga om de grundläggande rättigheterna och EU-domstolens anknutna rättspraxis, i synnerhet i ljuset av avgörandet i målet om direktivet om integritet och elektronisk kommunikation (2002/58/EG) och det anknutna målet beträffande La Quadrature du Net.

Unionsdomstolens avgöranden i anknytning till detta ämne (bland annat Digital Rights Ireland (C-293/12 och C-594/12), Schrems (C-362/14) och Tele2 Sverige och Watson (C-698/15 ja C-203/15)) gäller allmän och ospecificerad insamling av identifieringsuppgifter och lagring av dessa för myndighetssyften. Den nu aktuella propositionen handlar om uppgifter som myndigheterna själva samlat in och förvarat, vars inhämtning och lagring avgränsas fysiskt, tekniskt, kvantitativt och tidsmässigt. Utöver de grundläggande principerna har unionsdomstolens avgöranden inte konsekvenser för de nu framlagda lagförslagen.

10.7 Sammandrag

Den föreslagna regleringen innehåller exakta bestämmelser. Det väsentliga innehållet i begränsningen av de grundläggande fri- och rättigheterna framgår direkt av lagen. De nya befogenheterna förutsätter ett domstolsbeslut. Sålunda uppfyller regleringen kraven på bestämmelser genom lag och noggrann avgränsning. Med tanke på proportionalitetskravet är det väsentligt att föremål för den föreslagna befogenhetsregleringen är sådan verksamhet som nämns i 4 § i lagen om militär underrättelseverksamhet. Dessutom har noggrant avgränsade bestämmelser redan tidigare utfärdats om en militärunderrättelsemyndighets befogenhet. Regleringens proportionalitet ska bedömas i förhållande till den gällande lagstiftningen, i synnerhet lagen om militär underrättelseverksamhet, lagen om behandling av personuppgifter inom Försvarsmakten och lagen om övervakning av underrättelseverksamheten.

Den lagstiftning som föreslås i denna proposition bedöms uppfylla de krav som ställs i Europadomstolens avgörandepraxis och grundlagsutskottets tolkningspraxis vad gäller iakttagande av de grundläggande och mänskliga rättigheterna.

De lagförslag som ingår i propositionen kan enligt regeringens uppfattning behandlas i vanlig lagstiftningsordning.

De lagförslag som anknyter till propositionen innehåller ny typ av reglering. Det kan anses att 33, 42, 61 a, 61 b, 62, 63, 66, 67 a, 67 b, 78 a och 89 a § i lagförslag 1 i propositionen är relevanta med tanke på grundlagen. Dessutom kan helheten i 18 a § i lagförslag 1 anses vara central (inklusive lagförslag 7 och 8).

På grund av detta och övriga konstitutionella aspekter anser regeringen att det är ändamålsenligt att riksdagen begär ett utlåtande av grundlagsutskottet om propositionen.

Kläm

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

1.

Lag

om ändring av lagen om militär underrättelseverksamhet

I enlighet med riksdagens beslut
upphävs i lagen om militär underrättelseverksamhet (590/2019) 43 § 3 mom., 74 § och 78 § 5 mom.,

ändras 11 § 2 mom., 15 § 1 mom., 18 §, 20 § 3 mom., 33 § 2 och 3 mom., 36 § 1 mom., 42 och 44 §, 45 § 1 och 4 mom., 51 § 3 mom., 53 § 1 mom., 55 § 3 mom., 62 § 2 och 3 mom., 64 och 66–68 §, rubriken för 69 § och 69 § 2 mom., 70 §, 71 § 2 mom., 77 § 1 mom., 82 § 1 och 2 mom., 85, 86, 89, 91, 93 och 94 §, rubriken för 9 kap., 96 §, 97 § 2 mom., 99 och 101 §, 104 § 2 mom. samt 111 § 1 mom., av dem 20 § 3 mom. sådant det lyder i lag 333/2025, och

fogas till lagen en ny 18 a §, till 33 § ett nytt 4 mom., till 36 § ett nytt 4 mom., till lagen nya 46 a och 46 b §, till 51 § ett nytt 4 mom., varvid det nuvarande 4 och 5 mom. blir 5 och 6 mom., till lagen nya 55 a, 56 a, 61 a och 61 b §, till 62 § ett nytt 4 mom., till 63 § ett nytt 3 mom., varvid det nuvarande 3 mom. blir 4 mom., till lagen nya 67 a, 67 b, 78 a, 89 a och 89 b § samt till 104 § ett nytt 3 mom. som följer:

11 §

Militärunderrättelsemyndigheter

Armén, Marinen och Flygvapnet får för utförande av ett underrättelseuppdrag använda sig av informationskällor och radiosignalspaning. Armén, Marinen och Flygvapnet är underställda militärunderrättelsemyndigheterna i den militära underrättelseverksamheten.

15 §

Samordning av underrättelseverksamheten

Den militära och den civila underrättelseverksamheten samordnas mellan republikens presidents kansli, statsrådets kansli, utrikesministeriet, försvarsministeriet och inrikesministeriet samt vid behov mellan andra ministerier och myndigheter.

18 §

Samarbete med andra myndigheter och med företag och andra sammanslutningar

Militärunderrättelsemyndigheterna ska enligt behov agera i samarbete med andra myndigheter för att den militära underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt. För att genomföra sitt uppdrag kan Militärunderrättelsemyndigheterna trots sekretessbestämmelserna till andra myndigheter lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten.

För att genomföra sitt uppdrag kan Militärunderrättelsemyndigheterna trots sekretessbestämmelserna till företag och andra sammanslutningar lämna ut identifieringsuppgifter som anknyter till sabotageprogram eller lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten.

Bestämmelser om utlämnande av information för brottsbekämpning finns i 6 kap.

Närmare bestämmelser om organiserandet av samarbetet mellan Militärunderrättelsemyndigheterna och andra myndigheter samt om vilka som ska delta i samarbetet och om deras uppgifter får utfärdas genom förordning av statsrådet.

18 a §

Samverkan med Gränsbevakningsväsendet

Utöver vad som föreskrivs i 18 § kan Gränsbevakningsväsendet genom beslut av en Militärunderrättelsemyndighet och på begäran av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vidta en enskild åtgärd som anknyter till användning av en metod för underrättelseinhämtning enligt 22, 26, 28, 30, 32, 41, 42, 54 och 56 §, om det är nödvändigt för utförande av ett underrättelseuppdrag. Beslut om vidtagande av den åtgärd som begäran gäller ska vid Gränsbevakningsväsendet fattas av en anhållningsberättigad tjänsteman. Gränsbevakningsväsendet ska på begäran av en Militärunderrättelsemyndighet utan obefogat dröjsmål avbryta en åtgärd som avses i detta moment.

Om Militärunderrättelsemyndigheterna inte har befogenheter att vidta den åtgärd som behövs för skötseln av ett underrättelseuppdrag, kan Gränsbevakningsväsendet på begäran av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman i samband med en uppgift som föreskrivs för Gränsbevakningsväsendet vidta sådana åtgärder som avses i 28 § i gränsbevakningslagen (578/2005) och som är nödvändiga med tanke på ett uppdrag inom den militära underrättelseinhämtningen. Den person som är föremål för åtgärden är skyldig att vara närvarande högst 12 timmar åt gången när åtgärder vidtas. Beslut om vidtagande av en åtgärd ska vid Gränsbevakningsväsendet fattas av chefen vid ett gränsövergångsställe eller en gränsbevakningsman med minst löjtnants grad.

Gränsbevakningsväsendet har genom beslut av en gränsbevakningsman som är chef vid ett gränsövergångsställe eller en gränsbevakningsman med minst löjtnants grad rätt att använda falska, vilseledande eller förtäckta uppgifter då, när det är nödvändigt för att förhindra att en i denna paragraf avsedd åtgärd avslöjas.

Gränsbevakningsväsendet ska lämna upptagningar och handlingar som fåtts genom en åtgärd som avses i denna paragraf obehandlade till Militärunderrättelsemyndigheten samt utplåna upptagningar och handlingar som uppkommit vid genomförandet av åtgärden, om inte behandlingen av uppgifterna behövs för utförande av andra uppgifter som föreskrivs för Gränsbevakningsväsendet. Militärunderrättelsemyndigheten svarar för granskningen av upptagningar och handlingar samt för andra uppgifter i anslutning till databehandlingen.

20 §

Internationellt samarbete

En behörig utländsk tjänsteman har genom 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 på finskt territorium delta i användningen av metoder för underrättelseinhämtning. En utländsk tjänsteman är skyldig att iaktta de föreskrifter, begränsningar och anvisningar som militärunderrättelsemyndigheten meddelar.

33 §

Beslut om teknisk observation av utrustning

Tillstånd får beviljas för högst sex månader åt gången. När åtgärden gäller en person får tillstånd beviljas för högst tre 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 eller den person som använder den tekniska anordningen eller programvaran,
- 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.

Beslut om de tekniska anordningar eller den programvara som åtgärden riktas mot ska fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman, om åtgärden gäller en person. I beslutet ska valet av de anordningar eller den programvara som åtgärden riktas mot motiveras.

36 §

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. Om ett ärende som gäller teleavlyssning eller inhämtande av information i stället för teleavlyssning 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 att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

Beslut om de teleadresser eller den teleterminalutrustning som åtgärden riktas mot ska fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman, om åtgärden gäller en person. I beslutet ska valet av de teleadresser eller den teleterminalutrustning som åtgärden riktas mot motiveras.

42 §

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, teknisk observation av utrustning, underrättelseinhämtning som avser statliga aktörers datasystem eller underrättelseinhämtning som avser utländska datasystem på eller i föremål, ämnen, egendom, utrymmen, platser av annat slag eller informationssystem, 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 ovannämnda 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 får inte installeras eller avinstalleras i utrymmen som används för boende av permanent natur.

På begäran av en militärunderrättelsemyndighet har en person som inte hör till myndigheten rätt att under uppsikt och övervakning av en tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning vidta en i 1 mom. avsedd enskild installations- eller avinstallationsåtgärd som användningen av en metod för underrättelseinhämtning förutsätter, om det är nödvändigt för att kunna använda metoden för underrättelseinhämtning.

En militärunderrättelsemyndighet har rätt att för att installera eller avinstallera en metod eller programvara och för att överföra information, med datatekniska metoder tillfälligt använda en enskilds eller en sammanslutnings anordning eller del av informationssystem, om det är nödvändigt för att kunna använda metoden för underrättelseinhämtning. Militärunderrättelsemyndigheten får inte orsaka den anordning eller det informationssystem som används mer än ringa olägenhet eller skada. Militärunderrättelsemyndigheten är skyldig att ersätta mer än ringa olägenhet eller skada som den orsakat.

44 §

Plan för en täckoperation

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.

45 §

Beslut om en täckoperation

Beslut om en täckoperation ska fattas av huvudstabens underrättelsechef.

Vid förändrade omständigheter ska beslutet vid behov ses över.

46 a §

Täckoperation som genomförs uteslutande i datanät

Med täckoperation som genomförs uteslutande i datanät avses sådant planmässigt inhämtande av information om i 4 § avsedd verksamhet som genomförs i datanät 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 i ett datanät, om detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

Över en täckoperation som genomförs uteslutande i datanät ska en sådan skriftlig plan göras upp som innehåller väsentlig och tillräckligt detaljerad information för beslutsfattandet och genomförandet av täckoperationen. Vid förändrade omständigheter ska planen vid behov ses över.

46 b §

Beslut om en täckoperation som genomförs uteslutande i datanät

Beslut om en täckoperation som genomförs uteslutande i 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 som genomförs uteslutande i datanät får meddelas för högst sex månader åt gången.

Beslut om täckoperation som genomförs uteslutande i datanät ska fattas skriftligen.

I beslutet ska följande nämnas:

- 1) det underrättelseuppdrag som ligger till grund för åtgärden,
- 2) den person eller, i det fall att en bestämd person inte kan specificeras, grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information,
- 3) de fakta som den täckoperation som genomförs uteslutande i datanät grundar sig på,
- 4) beslutets giltighetstid med angivande av klockslag,
- 5) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar den täckoperation som genomförs uteslutande i datanät,
- 6) eventuella begränsningar och villkor för den täckoperation som genomförs uteslutande i datanät.

Vid förändrade omständigheter ska beslutet vid behov ses över.

51 §

Användning av informationskällor

Vid styrd användning av informationskällor får en informationskälla inte ombes inhämta information på ett sådant sätt som förutsätter utövande av myndighetsbefogenheter.

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. Vid styrd användning av informationskällor får en informationskälla inte ombes inhämta information på ett sådant sätt som äventyrar informationskällans eller någon annan persons liv eller hälsa. Informationskällans säkerhet ska vid behov tryggas under och efter informationsinhämtningen.

53 §

Beslut om styrd användning av informationskällor

Beslut om styrd användning av informationskällor ska fattas av huvudstabens underrättelsechef eller en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

55 §

Beslut om platsspecifik underrättelseinhämtning

Beslut om platsspecifik underrättelseinhämtning som riktas mot ett fortskaffningsmedel och 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.

55 a §

Provtagning vid platsspecifik underrättelseinhämtning

Militärunderrättelsemyndigheterna har rätt att vid platsspecifik underrättelseinhämtning ta prov av ett ämne, egendom eller ett föremål, om det behövs för utförande av ett underrättelseuppdrag.

56 a §

Tillfälligt omhändertagande av ämnen, egendom eller föremål

Om provtagning enligt 55 a § eller kopiering enligt 56 § nödvändigt kräver det, har militärunderrättelsemyndigheterna rätt att tillfälligt omhänderta ett ämne, egendomen eller ett föremål. Ämnet, egendomen eller föremålet ska utan dröjsmål återlämnas när syftet med omhändertagandet har uppnåtts.

61 a §

Underrättelseinhämtning i hemlandet som avser statliga aktörers datasystem

Med underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem avses att information inhämtas på finskt territorium från den del av ett datasystem som en statlig aktör administrerar eller använder i Finland, som genomför eller främjar den verksamhet som är föremål för ett underrättelseuppdrag eller lagrar eller förmedlar information som hänför sig till den verksamhet som är föremål för ett underrättelseuppdrag.

Underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem får användas endast i den omfattning som är nödvändig för att inhämta information om den verksamhet som är föremål för ett underrättelseuppdrag.

61 b §

Beslut om underrättelseinhämtning i hemlandet som avser statliga aktörers datasystem

Beslut om underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem ska fattas av domstol på yrkande av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Tillstånd till underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem får beviljas för högst sex månader åt gången.

I ett yrkande och i ett beslut om underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem ska följande nämnas:

- 1) underrättelseuppdraget,
- 2) den statliga aktör som är föremål för åtgärden och det datasystem som aktören använder,
- 3) de fakta som förutsättningarna för och inriktningen av underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem grundar sig på,
- 4) giltighetstiden med angivande av klockslag för tillståndet till underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem,
- 5) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem,
- 6) eventuella begränsningar och villkor för underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem.

Beslut om de teleadresser eller den teleterminalutrustning eller de anordningar eller den programvara som åtgärden riktas mot under giltighetstiden för tillståndet för metoden för underrättelseinhämtning ska fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. I beslutet ska valet av de teleadresser eller den teleterminalutrustning eller de anordningar eller den programvara som åtgärden riktas mot motiveras.

62 §

Underrättelseinhämtning som avser utländska datasystem

Militärunderrättelsemyndigheterna 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 och de åtgärder som hänför sig till underrättelseinhämtningen. Vid förändrade omständigheter ska planen vid behov ses över.

Militärunderrättelsemyndigheterna har som en del av underrättelseinhämtning som avser utländska datasystem rätt att vidta behövliga datatekniska åtgärder enligt internationell rätt i ett datasystem utanför finskt territorium, om Finlands försvar eller den nationella säkerheten kan orsakas allvarlig fara med datasystemet eller med hjälp av det. Åtgärderna ska vara nödvändiga, proportionerliga och tillfälliga.

63 §

Beslut om underrättelseinhämtning som avser utländska datasystem

Beslut om åtgärder enligt 62 § 4 mom. ska fattas av huvudstabens underrättelsechef. Innan huvudstabens underrättelsechef fattar beslut ska ärendet förberedelsevis behandlas mellan de

myndigheter som avses i 15 § 1 mom. och vid behov ska riktlinjer för ärendet dras upp vid det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president.

64 §

Militär underrättelseinhämtning utomlands

Vid militär underrättelseinhämtning utomlands och vid användning av metoder för underrättelseinhämtning utomlands får tillämpning av bestämmelserna i 12 § 3 mom., 51 § 3 mom., 60 § 3 mom. och 85 § 2 mom. frångås i enskilda fall, om det är nödvändigt. Bestämmelserna i 79, 80 och 89 § tillämpas inte på militär underrättelseinhämtning utomlands eller användning av metoder för underrättelseinhämtning utomlands.

Beslut om militär underrättelseinhämtning utomlands och om tillåtna metoder för underrättelseinhämtningen ska fattas av huvudstabens underrättelsechef. En med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman beslutar om användning av en i beslutet avsedd enskild metod för underrättelseinhämtning.

Deltagande i sådan militär underrättelseinhämtning utomlands som avses i denna paragraf förutsätter samtycke av den berörda tjänstemannen vid en militärunderrättelsemyndighet.

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.

66 §

Behandling av tekniska data för identifiering av en del av ett kommunikationsnät och för identifiering av dirigeringen av och ändringar i datatrafiken

Försvarsmaktens underrättelsetjänst får i datatrafiken i ett kommunikationsnät samla in och lagra tekniska data om datatrafiken och med hjälp av automatisk databehandling behandla dem

1) för statistisk analys i syfte att inrikta underrättelseinhämtning som avser datatrafik på en del av kommunikationsnätet,

2) för övervakning av dirigeringen av och ändringar i datatrafiken.

I verksamhet som avses i 1 mom. får det inte skapas information genom vilken en enskild fysisk person kan identifieras.

De tekniska data som avses i denna paragraf får lagras i högst 18 månader. Mängden tekniska data som lagras får inte överstiga fem procent av kapaciteten i den del av ett kommunikationsnät som överskrider Finlands gräns som är föremål för datainsamlingen. Lagrade data får användas för de ändamål som anges i 1 mom. och nedan i denna lag.

Försvarsmaktens underrättelsetjänst ska utplåna insamlade och lagrade tekniska data om datatrafiken senast efter att den lagringstid som föreskrivs i 3 mom. har gått ut.

67 §

Beslut om behandling av tekniska data för identifiering av en del av ett kommunikationsnät och för identifiering av dirigeringen av och ändringar i datatrafiken

Beslut om behandling av tekniska data för identifiering av en del av ett kommunikationsnät eller för identifiering av dirigeringen av och ändringar i datatrafiken 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 får beviljas och beslut fattas för högst sex månader åt gången räknat från den dag då tillståndet beviljas eller beslutet fattas, och tillståndet eller beslutet kan gälla även i 66 § 3 mom. avsedda lagrade data.

I ett yrkande och i ett beslut ska följande nämnas:

- 1) det geografiska område eller nätområde i fråga om vilket tekniska data i inkommande eller utgående datatrafik ska behandlas, eller föremålet för övervakningen av dirigeringen av och ändringar i datatrafiken,
- 2) de delar av kommunikationsnätet där data söks,
- 3) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar behandlingen,
- 4) en plan för hur behandlingen ska genomföras.

67 a §

Underrättelseinhämtning som avser datatrafik för fastställande av sökbegrepp

Försvarsmaktens underrättelsetjänst får samla in och lagra datatrafik i en del av ett kommunikationsnät som överskrider Finlands gräns i syfte att noggrannare inrikta underrättelseinhämtning som avser datatrafik och fastställa sökbegrepp på basis av de förmodade regelbundenheterna eller särdragen i den datatrafik som är föremål för den militära underrättelseinhämtningen.

Vid fastställandet av sökbegrepp ska behandlingen av datatrafiken ske i den maskinläsbara formen för datatrafiken. Vid fastställandet av sökbegrepp får uppgifter i ett meddelandes betydelseinnehåll inte utnyttjas. Som resultat av fastställandet av sökbegrepp får det inte uppstå information som beskriver ett meddelandes innehåll eller information utifrån vilken det kan dras slutsatser om en persons privatliv.

Mängden datatrafik som samlas in och lagras får inte överstiga fem procent av kapaciteten i den del av ett kommunikationsnät som överskrider Finlands gräns som är föremål för insamlingen. Den insamlade och lagrade datatrafiken får bevaras i högst tolv månader. Lagrade data får användas för de ändamål som anges i 1 mom. och nedan i denna lag.

Vid fastställandet av sökbegrepp får tekniska data som lagrats med stöd av 66 § 3 mom. användas.

Försvarsmaktens underrättelsetjänst ska utplåna insamlade och lagrade tekniska data om datatrafiken senast efter att den lagringstid som avses i 3 mom. har gått ut.

67 b §

Beslut om fastställande av sökbegrepp

Beslut om fastställande av sökbegrepp 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 får beviljas och beslut fattas för högst sex månader åt gången räknat från den dag då tillståndet beviljas eller beslutet fattas, och tillståndet eller beslutet kan gälla även i 66 § 3 mom. och 67 a § 3 mom. avsedda lagrade data.

I ett yrkande och i ett beslut ska följande nämnas:

- 1) det underrättelseuppdrag för vilket sökbegrepp fastställs och de fakta som gäller det,
- 2) de fakta som nödvändigheten av fastställandet av sökbegrepp grundar sig på,
- 3) de förmodade regelbundenheter eller särdrag i objektets datatrafik på basis av vilka sökbegreppen fastställs, och motiveringarna till sådana förmodanden,

- 4) de delar av kommunikationsnätet där data söks,
- 5) en plan för hur sökbegreppen ska fastställas,
- 6) tillståndets giltighetstid med angivande av klockslag,
- 7) den med användningen av Försvarsmaktens underrättelsetjänsts metoder för underrättelseinhämtning särskilt förtroga tjänsteman som leder och övervakar fastställandet av sökbegrepp,
- 8) eventuella begränsningar och villkor för fastställandet av sökbegrepp.

68 §

Underrättelseinhämtning som avser datatrafik hos statliga aktörer

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 aktör och dennes datatrafik samt behandla en sådan aktörs kommunikation. Inhämtningen av information i datatrafiken grundar sig på användningen av sökbegrepp som beskriver den statliga aktören.

Försvarsmaktens underrättelsetjänst får behandla den information som inhämtats i datatrafiken automatiskt och manuellt.

Som sökbegrepp får tillfälligt användas uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland.

Sådan informationsinhämtning som avses i denna paragraf kan också riktas mot data som lagrats med stöd av 66 § 3 mom. och 67 a § 3 mom.

69 §

Beslut om underrättelseinhämtning som avser datatrafik hos statliga aktörer

Tillstånd får beviljas och beslut fattas för högst sex månader åt gången räknat från den dag då tillståndet beviljas eller beslutet fattas, och tillståndet eller beslutet kan gälla även i 66 § 3 mom. och 67 a § 3 mom. avsedda lagrade data.

70 §

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 informationen inte kan erhållas genom någon annan metod för underrättelseinhämtning. Inhämtningen av information i datatrafiken grundar sig på användningen av sökbegrepp.

Som sökbegrepp får tillfälligt användas uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland.

Vid inriktningen av underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer får sökbegrepp som riktas mot ett meddelandes innehåll användas. Språkliga uttryck får användas som sökbegrepp endast tillsammans med tekniska data.

Försvarsmaktens underrättelsetjänst får behandla den information som inhämtats i datatrafiken automatiskt och manuellt.

Sådan informationsinhämtning som avses i denna paragraf kan också riktas mot data som lagrats med stöd av 66 § 3 mom. och 67 a § 3 mom.

71 §

Beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer

Tillstånd får beviljas och beslut fattas för högst sex månader åt gången räknat från den dag då tillståndet beviljas eller beslutet fattas, och tillståndet eller beslutet kan gälla även i 66 § 3 mom. och 67 a § 3 mom. avsedda lagrade data.

77 §

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 eller ett utrymme som ska användas i sådan verksamhet ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att tjänstemannens säkerhet ska kunna tryggas.

78 a §

Tryggande av informationskällans liv och hälsa

Genom beslut av huvudstabens underrättelsechef får militärunderrättelsemyndigheterna ge en informationskälla falska, vilseledande och förtäckta uppgifter eller registeranteckningar, som får användas i ett enskilt fall, eller falska handlingar som 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 föreligger.

Genom beslut av huvudstabens underrättelsechef får militärunderrättelsemyndigheterna ordna att informationskällan kommer till Finland, om det är nödvändigt för att skydda informationskällans liv och hälsa och om förfarandet som helhet bedömt kan anses vara försvarbart.

Informationskällan har rätt att komma in i landet i en situation som avses i 2 mom. och att i samband med inresan använda sådana falska uppgifter, anteckningar och handlingar som avses i 1 mom.

82 §

Förbud mot underrättelseinhämtning

Teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning, optisk observation, teknisk observation av utrustning, radiosignalspaning, underrättelseinhämtning i Finland som avser en statlig aktörs datasystem eller

underrättelseinhämtning som avser datatrafik 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 eller 20 § eller 22 § 2 mom. i rättegångsbalken.

Om det under tiden för teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning, optisk observation, teknisk observation av utrustning, radiosignalspaning, underrättelseinhämtning i Finland som avser en statlig aktörs datasystem 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 omedelbart utplånas.

85 §

Avbrytande av användningen av en metod för underrättelseinhämtning

Om det framgår att teleavlyssningen eller teleövervakningen riktas mot något annat meddelande än ett meddelande från eller till den person 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, ska användningen av metoden för underrättelseinhämtning till denna del avbrytas så snart det är möjligt, och de upptagningar som fåtts genom avlyssningen, de uppgifter som har fåtts genom teleövervakningen och anteckningarna om de uppgifter som fåtts genom användningen av sådana metoder för underrättelseinhämtning genast utplånas.

Skyldigheten att avbryta åtgärden och att utplåna upptagningarna och anteckningarna gäller radiosignalspaning, om det framgår att radiosignalspaningen gäller innehållet i ett meddelande från någon annan än en statlig aktör.

Skyldigheten att avbryta åtgärden och att utplåna upptagningarna och anteckningarna gäller också teknisk observation av utrustning, om det framgår att observationen riktas mot ett förtroligt meddelande som omfattas av de bestämmelser i 4 kap. som gäller teleavlyssning, teleövervakning och annan teknisk observation än observation av utrustning eller om det framgår att den person som åtgärden riktas mot inte använder den anordning eller den programvara som är föremål för observationen.

Om det framgår att underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem riktas mot sådan databehandlingsutrustning, utrustning för dataöverföring eller programvara för databehandling som inte hör till det datasystem som tillståndet gäller, ska den underrättelseinhämtning i hemlandet som avser den statliga aktörens datasystem till denna del avbrytas så snart det är möjligt och de upptagningar och uppgifter som fåtts genom underrättelseinhämtningen och anteckningarna om uppgifterna genast utplånas.

Om det medan platsspecifik underrättelseinhämtning pågår framgår att underrättelseinhämtningen har riktats mot information om vilken det enligt 17 kap. 11, 13, 14, 16, 20 eller 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. Annan information än sådan som avses i detta moment får dock bevaras och lagras, om den behövs i de fall som anges i 79 eller 80 §.

86 §

Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik

Utöver vad som föreskrivs i 82 § 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,
 - 2) avsändaren, mottagaren eller den som upptar kommunikationen har skyldighet eller rätt att vägra vittna om informationen med stöd av de bestämmelser som nämns i 82 § 1 mom.,
 - 3) informationen inte behövs för landets försvar eller för att skydda den nationella säkerheten.
- För utlåningen svarar militärunderrättelsemyndigheterna. Om Försvarsmaktens underrättelsetjänst har lämnat uppgifterna till skyddspolisens vid ett tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning, svarar skyddspolisens för utlåningen.

89 §

Skyldighet att underrätta

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 efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts.

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 eller kopiering av en försändelse som riktas mot annat än ett meddelande, om förundersökning inte har inletts i ärendet utifrån en i 79 eller 80 § avsedd anmälan. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen (806/2011) iakttas.

När en fråga enligt 10 kap. 60 § 3 mom. i tvångsmedelslagen om att skjuta upp eller avstå från underrättelsen om användning av en metod för underrättelseinhämtning behandlas, ska yrkandet framställas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Den som varit föremål för användningen av en metod för underrättelseinhämtning behöver inte underrättas om detta, om föremålet har varit en statlig aktör.

89 a §

Underrättelse om användning av underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer

Den som varit föremål för underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer underrättas inte om användningen av metoden för underrättelseinhämtning.

En part som med stöd av 17 kap. 13, 14, 16 eller 20 § eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om information ska underrättas om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer, om information som omfattas av rätt eller skyldighet att vägra vittna har kommit fram i samband med den underrättelseinhämtning som avser datatrafik. Skyldighet att underrätta personen föreligger emellertid inte, om den information som inhämtats genom underrättelseinhämtning som avser datatrafik har utplånats med stöd av 85 eller 86 §.

89 b §

Lämnande och uppskjutande av samt avstående från underrättelse

En underrättelse till en person som avses i 89 § eller 89 a § 2 mom. ska göras skriftligen utan dröjsmål efter det att syftet med användningen av en ovan avsedd metod för underrättelseinhämtning har nåtts. De personer som avses i de bestämmelserna ska dock underrättas om användningen av metoden för underrättelseinhämtning senast ett år efter det att användningen av metoden för underrättelseinhämtning upphörde.

Om den som varit föremål för inhämtande av information inte är identifierad eller personens bostadsort i Finland inte är känd vid utgången av den tidsfrist eller det uppskjutande som avses i denna paragraf, ska personen utan obefogat dröjsmål skriftligen underrättas om användningen av metoden för underrättelseinhämtning så snart personens identitet och bostadsort i Finland har utretts.

Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om den underrättelse som getts till den som varit föremål för underrättelseinhämtning.

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 en underrättelse enligt 89 § 1 mom. och 89 a § 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 man helt får avstå från underrättelse, om det är nödvändigt med hänsyn till landets försvar eller för att skydda den nationella säkerheten eller liv eller hälsa.

I fråga om handläggning av underrättelseärenden i domstol ska 116 § iakttas.

91 §

Befogenheter för den som inte arbetar i tjänsteförhållande

En person som tjänstgör med stöd av värnpliktslagen (1438/2007) eller deltar i frivilliga övningar enligt 18 och 19 § i lagen om frivilligt försvar (556/2007) och som har fått tillräcklig utbildning får, för utförandet av ett underrättelseuppdrag, under ledning och övervakning av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman, använda de metoder för underrättelseinhämtning som avses i 4 kap., med undantag för styrd användning av informationskällor, täckoperationer och bevisprovokation genom köp.

En med användningen av metoder för underrättelseinhämtning särskilt förtrogen person som har tagit avsked från en militärunderrättelsemyndighet och som tjänstgör eller deltar i övningar enligt 1 mom. får under ledning och övervakning av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman använda de metoder för underrättelseinhämtning som avses i 4 kap.

93 §

Tjänsteansvar för den som inte arbetar i tjänsteförhållande

På en person som utför uppgifter enligt denna lag tillämpas bestämmelserna om straffrättsligt tjänsteansvar.

94 §

Skadeståndsansvar för den som inte arbetar i tjänsteförhållande

För en skada som en person som utför uppgifter enligt denna lag har orsakat svarar staten i enlighet med vad som föreskrivs i skadeståndslagen (412/1974).

På skadeståndsansvaret för den som deltar i frivilliga övningar enligt 18 och 19 § i lagen om frivilligt försvar tillämpas bestämmelserna om en värnpliktigs skadeståndsansvar i 4 kap. i skadeståndslagen när personen utför uppgifter enligt denna lag.

9 kap.

Yppandeförbud, skyldigheter och rättigheter som gäller kommunikationsförmedlare, leverantörer av datacentraltjänster och dataöverförare samt användning och erhållande av information

96 §

Biståndsskyldighet för kommunikationsförmedlare och leverantörer av datacentraltjänster

En kommunikationsförmedlare och en i 2 § 2 punkten i cybersäkerhetslagen (124/2025) avsedd leverantör av datacentraltjänster ska utan obefogat dröjsmål göra de kopplingar i ett kommunikationsnät eller en datacentraltjänst som behövs för teleavlyssning, teleövervakning och sådan underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem samt tillhandahålla militärunderrättelsemyndigheterna de uppgifter och redskap samt den personal som behövs för utförande av teleavlyssningen. Detsamma gäller även de situationer där en militärunderrättelsemyndighet genomför teleavlyssning, teleövervakning eller sådan underrättelseinhämtning i ett kommunikationsnät eller en datacentraltjänst i hemlandet som avser en statlig aktörs datasystem med hjälp av tekniska anordningar. Kommunikationsförmedlaren och leverantören av datacentraltjänster ska dessutom ge en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman sådana uppgifter som den har i sin besittning och som behövs för teknisk spårning.

Militärunderrättelsemyndigheten, den som utför åtgärden och den biträdande personalen har rätt att för att göra de kopplingar som behövs för teleavlyssning och för sådan underrättelseinhämtning i ett kommunikationsnät i hemlandet som avser en statlig aktörs datasystem få tillträde också till andra utrymmen än de som är i kommunikationsförmedlarens eller leverantörens av informationssamhällets tjänster besittning, dock inte till utrymmen som används för stadigvarande boende. En med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman beslutar om åtgärden.

97 §

Dataöverförares skyldighet att medverka till genomförandet och upprätthållandet av den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter

Om den accesspunkt som avses i 1 mom. inte kan genomföras med medverkan av dataöverföraren eller om det är nödvändigt för att skydda underrättelseinhämtning, har Försvarsmaktens underrättelsetjänst rätt att genomföra accesspunkten i den del av ett kommunikationsnät som dataöverföraren administrerar. Om inte skyddet för underrättelseinhämtning förutsätter något annat, ska dataöverföraren om möjligt vara på plats när den accesspunkt som förutsätts för den underrättelseinhämtning som avser datatrafik genomförs.

99 §

Ersättningar till kommunikationsförmedlare och leverantörer av datacentraltjänster

En kommunikationsförmedlare och leverantör av datacentraltjänster har rätt att så som föreskrivs i 299 § i lagen om tjänster inom elektronisk kommunikation få ersättning av statens medel för direkta kostnader som orsakats av att den i enlighet med 96 § har bistått en militärunderrättelsemyndighet och lämnat uppgifter. Beslut om betalning av ersättning fattas av den militärunderrättelsemyndighet som vidtagit åtgärden.

101 §

Sökande av ändring i ett ersättningsbeslut

Omprövning av ett beslut om ersättning till en kommunikationsförmedlare, leverantör av datacentraltjänster eller dataöverförare får begäras. Bestämmelser om begäran om omprövning finns i förvaltningslagen (434/2003).

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

Förvaltningsdomstolen ska ge Transport- och kommunikationsverket tillfälle att bli hört.

104 §

Rätt att få information av privata sammanslutningar

Militärunderrättelsemyndigheterna har i ett enskilt fall på begäran rätt att av kommunikationsförmedlare och leverantörer av datacentraltjänster få kontaktuppgifter för teleadresser som inte är upptagna i en offentlig katalog eller information som identifierar en teleadress eller teleterminalutrustning eller information som behövs för att identifiera en tjänsts användare eller abonnent, om informationen behövs för utförande av ett underrättelseuppdrag. Militärunderrättelsemyndigheterna har motsvarande rätt att få information om utdelningsadresser av en sammanslutning som bedriver postverksamhet.

Militärunderrättelsemyndigheterna har rätt att få de uppgifter som avses i denna paragraf utan dröjsmål och avgiftsfritt, om inte något annat föreskrivs i lag.

111 §

Undersökning av upptagningar

Upptagningar som uppkommit vid användningen av metoder för underrättelseinhämtning får undersökas endast av domstol och huvudstabens underrättelsechef, en till uppdraget av militärunderrättelsemyndigheterna förordnad tjänsteman eller av underrättelsetillsynsombudsmannen eller en av denne förordnad tjänsteman. Dessutom får upptagningar på förordnande av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman eller enligt anvisning av domstolen också undersökas av en annan än en ovan avsedd tjänsteman vid en militärunderrättelsemyndighet, en sakkunnig eller en annan person som bistår vid inhämtande av information.

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) nya 8 b och 8 c § samt till 36 a §, sådan den lyder i lag 890/2018, ett nytt 3 mom. som följer:

8 b §

Inhämtande av information från allmänt tillgängliga källor

Försvarsmakten får för skötseln av sina uppgifter inhämta och behandla information från allmänt tillgängliga källor.

Försvarsmakten har rätt att använda tekniska anordningar, metoder eller programvaror för att söka och lagra information som härrör från en i 1 mom. avsedd källa.

Försvarsmakten får vid skyddandet av den informationsinhämtning som avses i 1 mom. använda falska, vilseledande eller förtäckt uppgifter för att hemlighålla uppdraget.

Huvudstaben fattar beslut om de förvaltningsenheter inom Försvarsmakten som ska ha rätt att använda det skydd för informationsinhämtning som avses i 3 mom.

Chefen för en i 4 mom. avsedd förvaltningsenhet beslutar om det skydd för informationsinhämtning som avses i 3 mom.

8 c §

Utplåning av uppgifter som inhämtats från allmänt tillgängliga källor

Information som erhållits vid sådan informationsinhämtning som avses i 8 b § ska utplånas utan dröjsmål efter att det har framgått att informationen inte behövs för utförande av Försvarsmaktens uppgifter.

Bestämmelser om behandling av personuppgifter finns i lagen om behandling av personuppgifter inom Försvarsmakten (332/2019).

36 a §

Ledigförklarande av tjänster

När andra än i 1 eller 2 mom. avsedda tjänster eller tjänsteförhållanden tillsätts genom ett ansökningsförfarande, kan Försvarsmakten låta bli att meddela dem som sökt tjänsten eller tjänsteförhållandet namnen på de andra sökandena och namnet på den som har utnämnts, om uppgiftens art nödvändigt kräver det. Sökandena ska dock underrättas om att tjänsten eller tjänsteförhållandet har tillsatts, och i utnämningsbeslutet ska nämnas den tjänst eller det tjänsteförhållande som tillsätts, vilken myndighet som har fattat beslutet samt datum för utnämningen.

Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 17 kap. 7 § i strafflagen

I enlighet med riksdagens beslut

ändras i strafflagen (39/1889) 17 kap. 7 § 2 mom., sådant det lyder i lag 650/2004, som följer:

7 §

Riksgränsbrott

För riksgränsbrott döms inte en utlänning som med anledning av en sådan gärning som avses i 1 mom. avvisas eller utvisas och inte heller en utlänning som på grund av flyktingskap ansöker om asyl eller uppehållstillstånd i Finland. För riksgränsbrott döms inte heller en utlänning som har begått ett brott enligt 1 mom. till följd av att han eller hon har varit föremål för människohandel enligt 25 kap. 3 eller 3 a § eller som har begått en i 1 mom. avsedd gärning på grundval av 78 a § 3 mom. i lagen om militär underrättelseverksamhet.

Denna lag träder i kraft den 20 .

4.

Lag

om ändring av 71 d § i lagen om Finansinspektionen

I enlighet med riksdagens beslut

ändras i lagen om Finansinspektionen (878/2008) 71 d §, sådan den lyder i lag 276/2025, som följer:

71 d §

Rätt att lämna ut uppgifter till skyddspolis och militärunderrättelsemyndigheterna

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet har Finansinspektionen rätt att trots sekretessbestämmelserna på begäran lämna ut information till skyddspolis, om informationen är nödvändig för förebyggande av brott som hör till skyddspolisens verksamhetsområde och för skyddande av den nationella säkerheten mot verksamhet som utgör ett allvarligt hot mot den, samt till en militärunderrättelsemyndighet, om informationen är nödvändig med tanke på militärunderrättelsemyndighetens underrättelseuppdrag.

Finansinspektionen har rätt att trots sekretessbestämmelserna på eget initiativ till skyddspolis eller militärunderrättelsemyndighet lämna ut information som Finansinspektionen har i sin besittning gällande penningtvätt eller finansiering av terrorism,

kringgående av sanktionsbestämmelser eller andra ovanliga transaktioner genom vilka medel överförs till tredjeländer, om åtgärderna misstänks äventyra den nationella säkerheten och om informationen är behövlig för förebyggande av brott som hör till skyddspolisens verksamhetsområde och för skyddande av den nationella säkerheten mot verksamhet som allvarligt hotar den eller om informationen är behövlig med tanke på militärunderrättelsemyndighetens underrättelseuppdrag.

På utlämnande av den information som avses i 1 och 2 mom. tillämpas det som föreskrivs i 71 § 5 mom.

Denna lag träder i kraft den 20 .

5.

Lag

om ändring av 6 § i lagen om Enheten för utredning av grå ekonomi

I enlighet med riksdagens beslut
ändras i lagen om Enheten för utredning av grå ekonomi (1207/2010) 6 § 1 mom. 40 punkten, sådan den lyder i lag 24/2026, samt
fogas till 6 § 1 mom., sådant det lyder i lagarna 308/2016, 858/2016, 1159/2016, 1413/2016, 1419/2016, 324/2017, 454/2017, 1112/2017, 404/2018, 414/2018, 722/2019, 1399/2019, 624/2020, 488/2021, 690/2021, 1134/2021, 495/2022, 713/2022, 1119/2022, 1327/2022, 1340/2022, 1355/2022, 743/2023, 190/2024, 940/2024, 260/2025, 277/2025 och 24/2026, en ny 41 punkt som följer:

6 §

Syftet med fullgöranderapporter

Fullgöranderapporter utarbetas till stöd för

- 40) utredning av tillförlitlighet och lämplighet som det föreskrivs om i 10 § i penningspelslagen (10/2026),
41) militär underrättelseinhämtning som avses i lagen om militär underrättelseverksamhet (590/2019).

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av 92 b § i inkomstskattelagen

I enlighet med riksdagens beslut

ändras i inkomstskattelagen (1535/1992) 92 b § 3 punkten, sådan den lyder i lag 404/2025, som följer:

92 b §

Vittnesarvode, belöning för tips och arvode som betalas för användning av informationskälla

Skattepliktig inkomst är inte

3) arvode som en myndighet betalar en i lagen om militär underrättelseverksamhet (590/2019) och i polislagen (872/2011) avsedd informationskälla för inhämtande av för skötseln av ett underrättelseuppdrag betydelsefulla uppgifter eller för biträdande av en underrättelsemyndighet och en i lagen om brottsbekämpning inom Gränsbevakningsväsendet (108/2018) avsedd informationskälla för inhämtande av uppgifter som är av betydelse för skötseln av uppdrag som hänför sig till upprätthållandet av gränssäkerheten.

Denna lag träder i kraft den 20 .

7.

Lag

om ändring av gränsbevakningslagen

I enlighet med riksdagens beslut

ändras i gränsbevakningslagen (578/2005) 3 § 3 mom., sådant det lyder i lag 749/2014, och *fogas* till lagen en ny 25 a § som följer:

3 §

Gränsbevakningsväsendets uppgifter

Gränsbevakningsväsendet utför polis- och tulluppgifter, efterspanings- och räddningsuppgifter och prehospital akutsjukvård samt deltar i det militära försvaret och i militär underrättelseinhämtning. Bestämmelser om gränsbevakningsväsendets uppgifter inom området för sjöräddningstjänsten finns i sjöräddningslagen.

25 a §

Gränsbevakningsväsendets deltagande i militär underrättelseinhämtning

Gränsbevakningsväsendet deltar på en underrättelsemyndighets begäran i militär underrättelseinhämtning genom att inhämta information och genom att vidta åtgärder till stöd för militärunderrättelsemyndigheternas underrättelseuppdrag.

Bestämmelser om gränsbevakningsväsendets befogenheter vid deltagande i militär underrättelseinhämtning finns i lagen om militär underrättelseverksamhet (590/2019).

Denna lag träder i kraft den 20 .

8.

Lag

om ändring av 32 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet

I enlighet med riksdagens beslut
fogas till 32 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019), sådan paragrafen lyder i lag 430/2024, ett nytt 2 mom. som följer:

32 §

Utlämnande av personuppgifter till en annan behörig myndighet som avses i dataskyddslagen avseende brottmål

Gränsbevakningsväsendet får trots sekretessbestämmelserna lämna ut sådana uppgifter som avses i 15 b § till Försvarsmakten för skötseln av de uppgifter som anges i lagen om militär underrättelseverksamhet (590/2019).

Denna lag träder i kraft den 20 .

9.

Lag

om ändring av lagen om behandling av personuppgifter inom Försvarsmakten

I enlighet med riksdagens beslut
fogas till lagen om behandling av personuppgifter inom Försvarsmakten (332/2019) en ny 37 a § som följer:

37 a §

Militärunderrättelsemyndighetens rätt att upprätthålla sitt personregister

Om en personuppgiftsansvarig enligt någon annan lag har rätt att ur sitt personregister lämna ut personuppgifter till Försvarsmakten genom en teknisk anslutning eller som en datamängd trots sekretessbestämmelserna, får militärunderrättelsemyndigheten för att upprätthålla sitt informationssystem jämföra uppgifterna i personregistret i fråga med innehållet i sina registrerade personuppgifter. Onödiga uppgifter ska raderas utan dröjsmål efter det att jämförelsen har gjorts. Onödiga personuppgifter får inte registreras.

Om det föreskrivs att den nationella säkerheten eller landets försvar är det ursprungliga ändamålet med behandlingen av uppgifterna eller att landets försvar eller den nationella

säkerheten är ett annat ändamål än det ursprungliga, har militärunderrättelsemyndigheten dessutom trots sekretessbestämmelserna rätt att i sitt informationssystem jämföra en datamängd insamlad från ett annat informationssystem, om förfarandet är nödvändigt för att göra behandlingen av uppgifter möjlig i ett informationssystem med hög informationssäkerhetsnivå. Datamängden ska förstöras utan dröjsmål efter det att behovet av jämförelse har upphört. De uppgifter som insamlas för jämförelsen ska hållas åtskilda från övriga uppgifter som militärunderrättelsemyndigheten behandlar.

Denna lag träder i kraft den 20 . _____

Helsingfors den 4 juni.2026

Statsminister

Petteri Orpo

Försvarsminister Antti Häkkinen

1.

Lag

om ändring av lagen om militär underrättelseverksamhet

I enlighet med riksdagens beslut
upphävs i lagen om militär underrättelseverksamhet (590/2019) 43 § 3 mom., 74 § och 78 § 5 mom.,
ändras 11 § 2 mom., 15 § 1 mom., 18 §, 20 § 3 mom., 33 § 2 och 3 mom., 36 § 1 mom., 42 och 44 §, 45 § 1 och 4 mom., 51 § 3 mom., 53 § 1 mom., 55 § 3 mom., 62 § 2 och 3 mom., 64 och 66–68 §, rubriken för 69 § och 69 § 2 mom., 70 §, 71 § 2 mom., 77 § 1 mom., 82 § 1 och 2 mom., 85, 86, 89, 91, 93 och 94 §, rubriken för 9 kap., 96 §, 97 § 2 mom., 99 och 101 §, 104 § 2 mom. samt 111 § 1 mom., av dem 20 § 3 mom. sådant det lyder i lag 333/2025, och
fogas till lagen en ny 18 a §, till 33 § ett nytt 4 mom., till 36 § ett nytt 4 mom., till lagen nya 46 a och 46 b §, till 51 § ett nytt 4 mom., varvid det nuvarande 4 och 5 mom. blir 5 och 6 mom., till lagen nya 55 a, 56 a, 61 a och 61 b §, till 62 § ett nytt 4 mom., till 63 § ett nytt 3 mom., varvid det nuvarande 3 mom. blir 4 mom., till lagen nya 67 a, 67 b, 78 a, 89 a och 89 b § samt till 104 § ett nytt 3 mom. som följer:

Gällande lydelse

Föreslagen lydelse

11 §

11 §

Militärunderrättelsemyndigheter

Militärunderrättelsemyndigheter

Bestämmelser om militär underrättelseverksamhet i armén, marinen och flygvapnet finns i 60 §. Armén, marinen och flygvapnet är underställda militärunderrättelsemyndigheterna i den militära underrättelseverksamheten.

Armén, Marinen och Flygvapnet får för utförande av ett underrättelseuppdrag använda sig av informationskällor och radiosignalspaning. Armén, Marinen och Flygvapnet är underställda militärunderrättelsemyndigheterna i den militära underrättelseverksamheten.

15 §

15 §

Samordning av underrättelseverksamheten

Samordning av underrättelseverksamheten

Den militära och den civila underrättelseverksamheten samordnas mellan republikens president, statsrådets kansli, utrikesministeriet, försvarsministeriet och

Den militära och den civila underrättelseverksamheten samordnas mellan republikens presidents kansli, statsrådets kansli, utrikesministeriet, försvarsministeriet

Gällande lydelse

inrikesministeriet samt vid behov mellan andra ministerier och myndigheter.

18 §

Samarbete med andra myndigheter och med företag och andra 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, trots sekretessbestämmelserna lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten. *Bestämmelser om utlämnande av personuppgifter finns i lagen om behandling av personuppgifter inom Försvarsmakten.*

För att genomföra sitt uppdrag kan Militärunderrättelsemyndigheterna trots sekretessbestämmelserna till företag och andra sammanslutningar lämna ut identifieringsuppgifter som anknyter till sabotageprogram och som behövs för utvecklingen av metoder och system för underrättelseinhämtning eller lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är nödvändigt med avseende på Försvarsmaktens verksamhet eller för att skydda den nationella säkerheten.

I 79 och 80 § föreskrivs om utlämnande av information för brottsbekämpning.

Närmare bestämmelser om organiserandet av samarbetet mellan Militärunderrättelsemyndigheterna och andra myndigheter samt om vilka som ska delta i samarbetet och om deras uppgifter får utfärdas genom förordning av statsrådet.

(ny)

Föreslagen lydelse

och inrikesministeriet samt vid behov mellan andra ministerier och myndigheter.

18 §

Samarbete med andra myndigheter och med företag och andra sammanslutningar

Militärunderrättelsemyndigheterna ska enligt behov agera i samarbete med andra myndigheter för att den militära underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt. För att genomföra sitt uppdrag kan Militärunderrättelsemyndigheterna trots sekretessbestämmelserna till andra myndigheter lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten.

För att genomföra sitt uppdrag kan Militärunderrättelsemyndigheterna trots sekretessbestämmelserna till företag och andra sammanslutningar lämna ut identifieringsuppgifter som anknyter till sabotageprogram eller lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten.

Bestämmelser om utlämnande av information för brottsbekämpning finns i 6 kap.

Närmare bestämmelser om organiserandet av samarbetet mellan Militärunderrättelsemyndigheterna och andra myndigheter samt om vilka som ska delta i samarbetet och om deras uppgifter får utfärdas genom förordning av statsrådet.

18 a §

Samverkan med Gränsbevakningsväsendet

Utöver vad som föreskrivs i 18 § kan Gränsbevakningsväsendet genom beslut av en militärunderrättelsemyndighet och på begäran av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman vidta en enskild åtgärd som anknyter till inledande av användning av en metod för underrättelseinhämtning enligt 22, 26, 28, 30, 32, 41, 42, 54 och 56 §, om det är nödvändigt för utförande av ett underrättelseuppdrag. Beslut om vidtagande av den åtgärd som begäran gäller ska vid Gränsbevakningsväsendet fattas av en anhållningsberättigad tjänsteman. Gränsbevakningsväsendet ska på begäran av en militärunderrättelsemyndighet utan obefogat dröjsmål avbryta en åtgärd som avses i detta moment.

Om militärunderrättelsemyndigheterna inte har befogenheter att vidta den åtgärd som behövs för skötseln av ett underrättelseuppdrag, kan Gränsbevakningsväsendet på begäran av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman i samband med en uppgift som föreskrivs för Gränsbevakningsväsendet vidta sådana åtgärder som avses i 28 § i gränsbevakningslagen (578/2005) och som är nödvändiga med tanke på ett uppdrag inom den militära underrättelseinhämtningen. Den person som är föremål för åtgärden är skyldig att vara närvarande högst 12 timmar åt gången när åtgärder vidtas. Beslut om vidtagande av en åtgärd ska vid Gränsbevakningsväsendet fattas av chefen vid ett gränsövergångsställe eller en gränsbevakningsman med minst löjtnants grad.

Gränsbevakningsväsendet har genom beslut av en gränsbevakningsman som är chef vid ett gränsövergångsställe eller en gränsbevakningsman med minst löjtnants grad rätt att använda falska, vilseledande

Gällande lydelse

Föreslagen lydelse

eller förtäckta uppgifter då, när det är nödvändigt för att förhindra att en i denna paragraf avsedd åtgärd avslöjas.

Gränsbevakningsväsendet ska lämna upptagningar och handlingar som fåtts genom en åtgärd som avses i denna paragraf obehandlade till militärunderrättelsemyndigheten samt utplåna upptagningar och handlingar som uppkommit vid genomförandet av åtgärden, om inte behandlingen av uppgifterna behövs för utförande av andra uppgifter som föreskrivs för Gränsbevakningsväsendet. Militärunderrättelsemyndigheten svarar för granskningen av upptagningar och handlingar samt för andra uppgifter i anslutning till databehandlingen.

20 §

20 §

Internationellt samarbete

Internationellt samarbete

En behörig utländsk tjänsteman har genom 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 22, 24, 43, 47, 51, 60 och 66 §. En utländsk tjänsteman är skyldig att iaktta de föreskrifter, begränsningar och anvisningar som militärunderrättelsemyndigheten meddelar.

En behörig utländsk tjänsteman har genom 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 på finskt territorium delta i användningen av metoder för underrättelseinhämtning. En utländsk tjänsteman är skyldig att iaktta de föreskrifter, begränsningar och anvisningar som militärunderrättelsemyndigheten meddelar.

33 §

33 §

Beslut om teknisk observation av utrustning

Beslut om teknisk observation av utrustning

Tillstånd får beviljas för högst sex månader åt gången.

Tillstånd får beviljas för högst sex månader åt gången. När åtgärden gäller en person får tillstånd beviljas för högst tre månader åt gången.

Gällande lydelse

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 förtrogn tjänsteman som leder och övervakar den tekniska observationen av utrustning,

6) eventuella begränsningar och villkor för den tekniska observationen av utrustning.

(ny)

36 §

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.

Föreslagen lydelse

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 *eller den person som använder den tekniska anordningen eller programvaran,*

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 förtrogn tjänsteman som leder och övervakar den tekniska observationen av utrustning,

6) eventuella begränsningar och villkor för den tekniska observationen av utrustning.

Beslut om de tekniska anordningar eller den programvara som åtgärden riktas mot ska fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman, om åtgärden gäller en person. I beslutet ska valet av de anordningar eller den programvara som åtgärden riktas mot motiveras.

36 §

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. *Om ett ärende som gäller teleavlyssning eller inhämtande av information i stället för teleavlyssning 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 att domstolen har avgjort yrkandet*

Gällande lydelse

Föreslagen lydelse

om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

(ny)

Beslut om de teleadresser eller den teleterminalutrustning som åtgärden riktas mot ska fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman, om åtgärden gäller en person. I beslutet ska valet av de teleadresser eller den teleterminalutrustning som åtgärden riktas mot motiveras.

42 §

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 ovannämnda 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 får inte installeras eller avinstalleras i utrymmen som används för boende av permanent natur.

(ny)

42 §

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, teknisk observation av utrustning, *underrättelseinhämtning som avser statliga aktörers datasystem* eller *underrättelseinhämtning som avser utländska datasystem* på eller i föremål, ämnen, egendom, utrymmen, platser av annat slag eller informationssystem, 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 ovannämnda 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 får inte installeras eller avinstalleras i utrymmen som används för boende av permanent natur.
På begäran av en militärunderrättelsemyndighet har en person

Gällande lydelse

(ny)

43 §

Täckoperation

Med *täckoperation* avses planmässigt inhämtande av information om en person eller dennes verksamhet eller, i det fall att en bestämd person inte kan specificeras, 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 den verksamhet som är föremål för underrättelseuppdraget är planmässig, organiserad eller yrkesmässig

Föreslagen lydelse

som inte hör till myndigheten rätt att under uppsikt och övervakning av en tjänsteman som är särskilt förtrogen med användningen av metoder för underrättelseinhämtning vidta en i 1 mom. avsedd enskild installations- eller avinstallationsåtgärd som användningen av en metod för underrättelseinhämtning förutsätter, om det är nödvändigt för att kunna använda metoden för underrättelseinhämtning.

En militärunderrättelsemyndighet har rätt att för att installera eller avinstallera en metod eller programvara och för att överföra information, med datatekniska metoder tillfälligt använda en enskilds eller en sammanslutnings anordning eller del av informationssystem, om det är nödvändigt för att kunna använda metoden för underrättelseinhämtning.

Militärunderrättelsemyndigheten får inte orsaka den anordning eller del av informationssystem som används mer än ringa olägenhet eller skada. Militärunderrättelsemyndigheten är skyldig att ersätta mer än ringa olägenhet eller skada som den orsakat.

43 §

Täckoperation

Med *täckoperation* avses planmässigt inhämtande av information om en person eller dennes verksamhet eller, i det fall att en bestämd person inte kan specificeras, 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 den verksamhet som är föremål för underrättelseuppdraget är planmässig, organiserad eller yrkesmässig

Gällande lydelse

eller om det kan antas att verksamheten fortsätter eller upprepas.

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.

44 §

Framställning om och plan för en täckoperation

Peitetoimintaa koskevassa esityksessä on mainittava:

- 1) toimenpiteen esittäjä;*
- 2) tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä;*
- 3) toimenpiteen perusteena oleva tiedustelutehtävä;*
- 4) peitetoiminnan tavoite;*
- 5) peitetoiminnan tarpeellisuus;*
- 6) muut peitetoiminnan edellytysten arviointia varten tarvittavat tiedot.*

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.

45 §

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.*

Föreslagen lydelse

eller om det kan antas att verksamheten fortsätter eller upprepas.

(upphävs)

44 §

Plan för en täckoperation

(upphävs)

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.

45 §

Beslut om en täckoperation

Beslut om en täckoperation ska fattas av huvudstabens underrättelsechef.

Vid förändrade omständigheter ska beslutet vid behov ses över.

Gällande lydelse

Vid förändrade omständigheter ska beslutet vid behov ses över. *Beslut om avslutande av en täckoperation ska fattas skriftligen.*

Föreslagen lydelse

(ny)

46 a §

Täckoperation som genomförs uteslutande i datanät

Med täckoperation som genomförs uteslutande i datanät avses sådant planmässigt inhämtande av information om i 4 § avsedd verksamhet som genomförs i datanät 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 i ett datanät, om detta med fog kan antas vara av synnerlig vikt för att få information med avseende på ett underrättelseuppdrag.

Över en täckoperation som genomförs uteslutande i datanät ska en sådan skriftlig plan göras upp som innehåller väsentlig och tillräckligt detaljerad information för beslutsfattandet och genomförandet av täckoperationen. Vid förändrade omständigheter ska planen vid behov ses över.

(ny)

46 b §

Beslut om en täckoperation som genomförs uteslutande i datanät

Beslut om en täckoperation som genomförs uteslutande i datanät ska fattas av en för uppdraget förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Gällande lydelse

Föreslagen lydelse

Beslut om en täckoperation som genomförs uteslutande i datanät får meddelas för högst sex månader åt gången.

Beslut om täckoperation som genomförs uteslutande i datanät ska fattas skriftligen.

I beslutet ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,

2) den person eller, i det fall att en bestämd person inte kan specificeras, grupp av personer, tillräckligt specificerad, som är föremål för inhämtandet av information,

3) de fakta som den täckoperation som genomförs uteslutande i datanät grundar sig på,

4) beslutets giltighetstid med angivande av klockslag,

5) den med användningen av metoder för underrättelseinhämtning särskilt förtroga tjänsteman som leder och övervakar den täckoperation som genomförs uteslutande i datanät,

6) eventuella begränsningar och villkor för den täckoperation som genomförs uteslutande i datanät.

Vid förändrade omständigheter ska beslutet vid behov ses över.

51 §

Användning av informationskällor

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.

51 §

Användning av informationskällor

Vid styrd användning av informationskällor får en informationskälla inte ombes inhämta information på ett sådant sätt som förutsätter utövande av myndighetsbefogenheter.

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. Vid styrd användning av informationskällor får en informationskälla inte ombes inhämta information på ett sådant sätt som äventyrar informationskällans eller någon annan persons liv eller hälsa. Informationskällans

Gällande lydelse

Föreslagen lydelse

säkerhet ska vid behov tryggas under och efter informationsinhämtningen.

53 §

Beslut om styrd användning av informationskällor

Beslut om styrd användning av informationskällor ska fattas av huvudstabens underrättelsechef.

53 §

Beslut om styrd användning av informationskällor

Beslut om styrd användning av informationskällor ska fattas av huvudstabens underrättelsechef eller en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

55 §

Beslut om platsspecifik underrättelseinhämtning

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.

55 §

Beslut om platsspecifik underrättelseinhämtning

Beslut om platsspecifik underrättelseinhämtning som riktas mot ett fortskaffningsmedel och 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.

(ny)

55 a §

Provtagning vid platsspecifik underrättelseinhämtning

Militärunderrättelsemyndigheterna har rätt att vid platsspecifik underrättelseinhämtning ta prov av ett ämne, egendom eller ett föremål, om det behövs för utförande av ett underrättelseuppdrag.

(ny)

56 a §

Gällande lydelse

Föreslagen lydelse

*Tillfälligt omhändertagande av ämnen,
egendom eller föremål*

Om provtagning enligt 55 a § eller kopiering enligt 56 § nödvändigt kräver det, har militärunderrättelsemyndigheterna rätt att tillfälligt omhänderta ett ämne, egendomen eller ett föremål. Ämnet, egendomen eller föremålet ska utan dröjsmål återlämnas när syftet med omhändertagandet har uppnåtts.

(ny)

61 a §

*Underrättelseinhämtning i hemlandet som
avser statliga aktörers datasystem*

Med underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem avses att information inhämtas på finskt territorium från den del av ett datasystem som en statlig aktör administrerar eller använder i Finland, som genomför eller främjar den verksamhet som är föremål för ett underrättelseuppdrag eller lagrar eller förmedlar information som hänför sig till den verksamhet som är föremål för ett underrättelseuppdrag.

Underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem får användas endast i den omfattning som är nödvändig för att inhämta information om den verksamhet som är föremål för ett underrättelseuppdrag.

(ny)

61 b §

*Beslut om underrättelseinhämtning i
hemlandet som avser statliga aktörers
datasystem*

Beslut om underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem ska fattas av domstol på yrkande av en med användningen av metoder för

Gällande lydelse

Föreslagen lydelse

underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Tillstånd till underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem får beviljas för högst sex månader åt gången.

I ett yrkande och i ett beslut om underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem ska följande nämnas:

- 1) underrättelseuppdraget,*
- 2) den statliga aktör som är föremål för åtgärden och det datasystem som aktören använder,*
- 3) de fakta som förutsättningarna för och inriktningen av underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem grundar sig på,*
- 4) giltighetstiden med angivande av klockslag för tillståndet till underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem,*
- 5) den med användningen av metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem,*
- 6) eventuella begränsningar och villkor för underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem.*

Beslut om de teleadresser eller den teleterminalutrustning eller de anordningar eller den programvara som åtgärden riktas mot under giltighetstiden för tillståndet för metoden för underrättelseinhämtning ska fattas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman. I beslutet ska valet av de teleadresser eller den teleterminalutrustning eller de anordningar eller den programvara som åtgärden riktas mot motiveras.

62 §

*Underrättelseinhämtning som avser
utländska datasystem*

62 §

*Underrättelseinhämtning som avser
utländska datasystem*

Gällande lydelse

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. Vid förändrade omständigheter ska planen vid behov ses över.

(ny)

63 §

Beslut om underrättelseinhämtning som avser utländska datasystem

(ny)

64 §

Militär underrättelseinhämtning utomlands

Föreslagen lydelse

Militärunderrättelsemyndigheterna 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 och de åtgärder som hänför sig till underrättelseinhämtningen. Vid förändrade omständigheter ska planen vid behov ses över.

Militärunderrättelsemyndigheterna har som en del av underrättelseinhämtning som avser utländska datasystem rätt att vidta behövliga datatekniska åtgärder enligt internationell rätt i ett datasystem utanför finskt territorium, om Finlands försvar eller den nationella säkerheten kan orsakas allvarlig fara med datasystemet eller med hjälp av det. Åtgärderna ska vara nödvändiga, proportionerliga och tillfälliga.

63 §

Beslut om underrättelseinhämtning som avser utländska datasystem

Beslut om åtgärder enligt 62 § 4 mom. ska fattas av huvudstabens underrättelsechef. Innan huvudstabens underrättelsechef fattar beslut ska ärendet förberedelsevis behandlas mellan de myndigheter som avses i 15 § 1 mom. och vid behov ska riktlinjer för ärendet dras upp vid det gemensamma mötet mellan utrikes- och säkerhetspolitiska ministerutskottet och republikens president.

64 §

Militär underrättelseinhämtning utomlands

Gällande lydelse

Vid militär underrättelseinhämtning utomlands och vid användning av metoder för underrättelseinhämtning utomlands får tillämpning av bestämmelserna i 12 § 3 mom., 60 § 3 mom. och 85 § 2 mom. frångås i enskilda fall, om det är nödvändigt. Bestämmelserna i 79, 80 och 89 § tillämpas inte på militär underrättelseinhämtning utomlands eller användning av metoder för underrättelseinhämtning utomlands.

Beslut om militär underrättelseinhämtning och användning av metoder för underrättelseinhämtning som sker utanför Finland ska fattas av huvudstabens underrättelsechef. Deltagande i sådan militär underrättelseinhämtning utomlands som avses i denna paragraf förutsätter samtycke av den berörda tjänstemannen vid en militärunderrättelsemyndighet.

(ny)

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.

66 §

Behandling av tekniska data

För inriktning av underrättelseinhämtning som avser datatrafik får Försvarmaktens 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.

Föreslagen lydelse

Vid militär underrättelseinhämtning utomlands och vid användning av metoder för underrättelseinhämtning utomlands får tillämpning av bestämmelserna i 12 § 3 mom., 51 § 3 mom., 60 § 3 mom. och 85 § 2 mom. frångås i enskilda fall, om det är nödvändigt. Bestämmelserna i 79, 80 och 89 § tillämpas inte på militär underrättelseinhämtning utomlands eller användning av metoder för underrättelseinhämtning utomlands.

Beslut om militär underrättelseinhämtning utomlands och om tillåtna metoder för underrättelseinhämtningen ska fattas av huvudstabens underrättelsechef. En med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman beslutar om användning av en i beslutet avsedd enskild metod för underrättelseinhämtning.

Deltagande i sådan militär underrättelseinhämtning utomlands som avses i denna paragraf förutsätter samtycke av den berörda tjänstemannen vid en militärunderrättelsemyndighet.

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.

66 §

Behandling av tekniska data för identifiering av en del av ett kommunikationsnät och för identifiering av dirigeringen av och ändringar i datatrafiken

Försvarmaktens underrättelsetjänst får i datatrafiken i ett kommunikationsnät samla in och lagra tekniska data om datatrafiken och med hjälp av automatisk databehandling behandla dem

1) för statistisk analys i syfte att inrikta underrättelseinhämtning som avser datatrafik på en del av kommunikationsnätet,

2) för övervakning av dirigeringen av och ändringar i datatrafiken.

Gällande lydelse

I resultatet av den statistiska analysen får inte ingå sådan information genom vilken en enskild fysisk person kan identifieras.
(ny)

Försvarsmaktens underrättelsetjänst ska förstöra insamlade och lagrade tekniska data om datatrafiken omedelbart efter att resultatet av den statistiska analysen har blivit klart.

67 §

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,

Föreslagen lydelse

I verksamhet som avses i 1 mom. får det inte skapas information genom vilken en enskild fysisk person kan identifieras.

De tekniska data som avses i denna paragraf får lagras i högst 18 månader. Mängden tekniska data som lagras får inte överstiga fem procent av kapaciteten i den del av ett kommunikationsnät som överskrider Finlands gräns som är föremål för datainsamlingen. Lagrade data får användas för de ändamål som anges i 1 mom. och nedan i denna lag.

Försvarsmaktens underrättelsetjänst ska utplåna insamlade och lagrade tekniska data om datatrafiken senast efter att den lagringstid som föreskrivs i 3 mom. har gått ut.

67 §

Beslut om behandling av tekniska data för identifiering av en del av ett kommunikationsnät och för identifiering av dirigeringen av och ändringar i datatrafiken

Beslut om behandling av tekniska data för identifiering av en del av ett kommunikationsnät eller för identifiering av dirigeringen av och ändringar i datatrafiken 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 får beviljas och beslut fattas för högst sex månader åt gången räknat från den dag då tillståndet beviljas eller beslutet fattas, och tillståndet eller beslutet kan gälla även i 66 § 3 mom. avsedda lagrade data.

I ett yrkande och i ett beslut ska följande nämnas:

1) det geografiska område eller nätområde i fråga om vilket tekniska data i inkommande eller utgående datatrafik ska behandlas, eller föremålet för övervakningen av dirigeringen av och ändringar i datatrafiken,

Gällande lydelse

2) de delar av kommunikationsnätet där data söks,

3) *en* med användningen av *Försvarsmaktens* *underrättelsetjänsts* metoder för underrättelseinhämtning särskilt förtroigna tjänsteman som leder och övervakar behandlingen *av tekniska data*,

4) en plan för hur behandlingen av tekniska data ska genomföras.

(ny)

Föreslagen lydelse

2) de delar av kommunikationsnätet där data söks,

3) *den* med användningen av metoder för underrättelseinhämtning särskilt förtroigna tjänsteman som leder och övervakar behandlingen,

4) en plan för hur behandlingen ska genomföras

67 a §

Underrättelseinhämtning som avser datatrafik för fastställande av sökbegrepp

Försvarsmaktens underrättelsetjänst får samla in och lagra datatrafik i en del av ett kommunikationsnät som överskrider Finlands gräns i syfte att noggrannare inrikta underrättelseinhämtning som avser datatrafik och fastställa sökbegrepp på basis av de förmodade regelbundenheterna eller särdragen i den datatrafik som är föremål för den militära underrättelseinhämtningen.

Vid fastställandet av sökbegrepp ska behandlingen av datatrafiken ske i den maskinläsbara formen för datatrafiken. Vid fastställandet av sökbegrepp får uppgifter i ett meddelandes betydelseinnehåll inte utnyttjas. Som resultat av fastställandet av sökbegrepp får det inte uppstå information som beskriver ett meddelandes innehåll eller information utifrån vilken det kan dras slutsatser om en persons privatliv.

Mängden datatrafik som samlas in och lagras får inte överstiga fem procent av kapaciteten i den del av ett kommunikationsnät som överskrider Finlands gräns som är föremål för insamlingen. Den insamlade och lagrade datatrafiken får bevaras i högst tolv månader. Lagrade data får användas för de ändamål som anges i 1 mom. och nedan i denna lag.

Vid fastställandet av sökbegrepp får tekniska data som lagrats med stöd av 66 § 3 mom. användas.

Försvarsmaktens underrättelsetjänst ska utplåna insamlade och lagrade tekniska data

Gällande lydelse

(ny)

Föreslagen lydelse

om datatrafiken senast efter att den lagringstid som avses i 3 mom. har gått ut.

67 b §

Beslut om fastställande av sökbegrepp

Beslut om fastställande av sökbegrepp 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 får beviljas och beslut fattas för högst sex månader åt gången räknat från den dag då tillståndet beviljas eller beslutet fattas, och tillståndet eller beslutet kan gälla även i 66 § 3 mom. och 67 a § 3 mom. avsedda lagrade data.

I ett yrkande och i ett beslut ska följande nämnas:

1) det underrättelseuppdrag för vilket sökbegrepp fastställs och de fakta som gäller det,

2) de fakta som nödvändigheten av fastställandet av sökbegrepp grundar sig på,

3) de förmodade regelbundenheter eller särdrag i objektets datatrafik på basis av vilka sökbegreppen fastställs, och motiveringarna till sådana förmodanden,

4) de delar av kommunikationsnätet där data söks,

5) en plan för hur sökbegreppen ska fastställas,

6) tillståndets giltighetstid med angivande av klockslag,

7) den med användningen av Försvarsmaktens underrättelsetjänsts metoder för underrättelseinhämtning särskilt förtrogna tjänsteman som leder och övervakar fastställandet av sökbegrepp,

8) eventuella begränsningar och villkor för fastställandet av sökbegrepp.

68 §

Underrättelseinhämtning som avser en statlig aktörs datatrafik

68 §

Underrättelseinhämtning som avser datatrafik hos statliga aktörer

Gällande lydelse

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.

(ny)

69 §

Beslut om underrättelseinhämtning som avser en statlig aktörs datatrafik

Tillstånd får beviljas för högst sex månader åt gången.

70 §

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

Föreslagen lydelse

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 aktör och dennes datatrafik samt behandla en sådan aktörs kommunikation. Inhämtningen av information i datatrafiken grundar sig på användningen av sökbegrepp som beskriver den statliga aktören.

Försvarsmaktens underrättelsetjänst får behandla den information som inhämtats i datatrafiken automatiskt och manuellt.

Som sökbegrepp får tillfälligt användas uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland.

Sådan informationsinhämtning som avses i denna paragraf kan också riktas mot data som lagrats med stöd av 66 § 3 mom. och 67 a § 3 mom.

69 §

Beslut om underrättelseinhämtning som avser datatrafik hos statliga aktörer

Tillstånd får beviljas och beslut fattas för högst sex månader åt gången räknat från den dag då tillståndet beviljas eller beslutet fattas, och tillståndet eller beslutet kan gälla även i 66 § 3 mom. och 67 a § 3 mom. avsedda lagrade data.

70 §

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

Gällande lydelse

underrättelseuppdrag, om informationen inte kan erhållas genom någon annan metod för underrättelseinhämtning. 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.

(ny)

71 §

Beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer

Tillstånd får beviljas för högst sex månader åt gången.

74 §

Utlämnande av uppgifter om ett skadligt datorprogram till företag och sammanslutningar

Militärunderrättelsemyndigheterna får trots sekretessbestämmelserna till ett företag, en sammanslutning eller myndighet lämna ut

Föreslagen lydelse

underrättelseuppdrag, om informationen inte kan erhållas genom någon annan metod för underrättelseinhämtning. Inhämtningen av information i datatrafiken grundar sig på användningen av sökbegrepp.

Som sökbegrepp får tillfälligt användas uppgifter som identifierar en teleterminalutrustning eller teleadress som innehas av eller annars förmodligen används av en person som vistas i Finland.

Vid inriktningen av underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer får sökbegrepp som riktas mot ett meddelandes innehåll användas. Språkliga uttryck får användas som sökbegrepp endast tillsammans med tekniska data.

Försvarsmaktens underrättelsetjänst får behandla den information som inhämtats i datatrafiken automatiskt och manuellt.

Sådan informationsinhämtning som avses i denna paragraf kan också riktas mot data som lagrats med stöd av 66 § 3 mom. och 67 a § 3 mom.

71 §

Beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer

Tillstånd får beviljas och beslut fattas för högst sex månader åt gången räknat från den dag då tillståndet beviljas eller beslutet fattas, och tillståndet eller beslutet kan gälla även i 66 § 3 mom. och 67 a § 3 mom. avsedda lagrade data.

(upphävs)

Gällande lydelse

Föreslagen lydelse

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.

77 §

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.

78 §

Tryggande av informationskällor

Huvudstabens underrättelsechef får besluta att en informationskälla ges, för användning i ett enskilt fall, falska, vilseledande och förtäckta uppgifter eller registeranteckningar 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 föreligger.

(ny)

77 §

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 *eller ett utrymme som ska användas i sådan verksamhet* ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att tjänstemannens säkerhet ska kunna tryggas.

78 §

Tryggande av informationskällor

78 a §

Tryggande av informationskällans liv och hälsa

Genom beslut av huvudstabens underrättelsechef får militärunderrättelsemyndigheterna ge en informationskälla falska, vilseledande och förtäckt uppgifter eller registeranteckningar, som får användas i ett enskilt fall, eller falska handlingar som 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 föreligger.

Genom beslut av huvudstabens underrättelsechef får militärunderrättelsemyndigheterna ordna att informationskällan kommer till Finland, om det är nödvändigt för att skydda informationskällans liv och hälsa och om förfarandet som helhet bedömt kan anses vara försvarbart.

Informationskällan har rätt att komma in i landet i en situation som avses i 2 mom. och att i samband med inresan använda sådana falska uppgifter, anteckningar och handlingar som avses i 1 mom.

82 §

Förbud mot underrättelseinhämtning

Teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning, optisk observation, radiosignalspaning eller underrättelseinhämtning som avser datatrafik 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 eller 20 § eller 22 § 2 mom. i rättegångsbalken.

Om det under tiden för teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning, optisk

82 §

Förbud mot underrättelseinhämtning

Teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning, optisk observation, *teknisk observation av utrustning*, radiosignalspaning, *underrättelseinhämtning i Finland som avser en statlig aktörs datasystem* eller underrättelseinhämtning som avser datatrafik 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 eller 20 § eller 22 § 2 mom. i rättegångsbalken.

Gällande lydelse

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.

Föreslagen lydelse

Om det under tiden för teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning, optisk observation, *teknisk observation av utrustning*, radiosignalspaning, *underrättelseinhämtning i Finland som avser en statlig aktörs datasystem* 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 *omedelbart* utplånas.

85 §

*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 radiosignalspaning, om det framgår att radiosignalspaningen gäller innehållet i ett meddelande från någon annan än en statlig aktör.

85 §

*Avbrytande av **användningen av en metod för underrättelseinhämtning***

Om det framgår att teleavlyssningen *eller teleövervakningen* riktas mot något annat meddelande än ett meddelande från eller till den person 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, ska användningen av metoden för underrättelseinhämtning till denna del avbrytas så snart det är möjligt, och de upptagningar som fåtts genom avlyssningen, *de uppgifter som har fåtts genom teleövervakningen* och anteckningarna om de uppgifter som fåtts genom *användningen av sådana metoder för underrättelseinhämtning* genast utplånas.

Skyldigheten att avbryta åtgärden och att utplåna upptagningarna och anteckningarna gäller radiosignalspaning, om det framgår att radiosignalspaningen gäller innehållet i ett meddelande från någon annan än en statlig aktör.

Gällande lydelse

Skyldigheten att avbryta åtgärden och att utplåna upptagningarna och anteckningarna gäller teknisk observation av utrustning, om det framgår att den person som avses i 32 § 4 mom. inte använder den anordning som är föremål för observationen.

(ny)

Om det medan platsspecifik underrättelseinhämtning pågår framgår att underrättelseinhämtningen har riktats mot information, om vilken det enligt 17 kap. 11, 13, 14, 16, 20 eller 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.

Annan information än sådan som avses i 4 mom. får dock bevaras och lagras, om den behövs i de fall som anges i 79 eller 80 §.

86 §

Föreslagen lydelse

Skyldigheten att avbryta åtgärden och att utplåna upptagningarna och anteckningarna gäller *också* teknisk observation av utrustning, om det framgår att *observationen riktas mot ett förtroligt meddelande som omfattas av de bestämmelser i 4 kap. som gäller teleavlyssning, teleövervakning och annan teknisk observation än observation av utrustning* eller om det framgår att den person som åtgärden riktas mot inte använder den anordning eller den programvara som är föremål för observationen.

Om det framgår att underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem riktas mot sådan databehandlingsutrustning, utrustning för dataöverföring eller programvara för databehandling som inte hör till det datasystem som tillståndet gäller, ska den underrättelseinhämtning i hemlandet som avser den statliga aktörens datasystem till denna del avbrytas så snart det är möjligt och de upptagningar och uppgifter som fås genom underrättelseinhämtningen och anteckningarna om uppgifterna genast utplånas.

Om det medan platsspecifik underrättelseinhämtning pågår framgår att underrättelseinhämtningen har riktats mot information om vilken det enligt 17 kap. 11, 13, 14, 16, 20 eller 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. *Annan information än sådan som avses i detta moment får dock bevaras och lagras, om den behövs i de fall som anges i 79 eller 80 §.*

86 §

Gällande lydelse

Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik

Utöver vad som föreskrivs i 82 § 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 nämns i 82 § 1 mom.

(ny)

För utplåningen svarar militärunderrättelsemyndigheterna. Om Försvarmaktens underrättelsetjänst har lämnat uppgifterna till skyddspolisen vid ett tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning, svarar skyddspolisen för utplåningen.

89 §

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

Föreslagen lydelse

Utplåning av information som inhämtats genom underrättelseinhämtning som avser datatrafik

Utöver vad som föreskrivs i 82 § 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,

2) avsändaren, mottagaren eller den som upptar kommunikationen har skyldighet eller rätt att vägra vittna om informationen med stöd av de bestämmelser som nämns i 82 § 1 mom.,

3) *informationen inte behövs för landets försvar eller för att skydda den nationella säkerheten.*

För utplåningen svarar militärunderrättelsemyndigheterna. Om Försvarmaktens underrättelsetjänst har lämnat uppgifterna till skyddspolisen vid ett tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning, svarar skyddspolisen för utplåningen.

89 §

Skyldighet att underrätta

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 efter det att syftet med användningen av metoden för underrättelseinhämtning har nåtts.

(upphävs)

för underrättelseinhämtning har nåtts och om identifieringsuppgifterna för eller innehållet i ett konfidentiellt meddelande från en person som vid tidpunkten för genomförandet av underrättelseinhämtningen befann sig i Finland har retts ut manuellt vid behandlingen. Skyldighet att underrätta personen föreligger emellertid inte, om den information som inhämtats genom underrättelseinhämtning som avser datatrafik har utplånats med stöd av 86 §.

Den som varit föremål för inhämtande av information ska dock underrättas om användningen av metoden för underrättelseinhämtning senast ett år efter 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.

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.

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 en underrättelse 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

Gällande lydelse

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 förundersökning inte har inletts i ärendet utifrån en i 79 eller 80 § avsedd anmälan. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen (806/2011) iakttas.

(ny)

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 116 § iakttas.

(ny)

Föreslagen lydelse

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 eller kopiering av en försändelse som riktas mot annat än ett meddelande, om förundersökning inte har inletts i ärendet utifrån en i 79 eller 80 § avsedd anmälan. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § 2–7 mom. i tvångsmedelslagen (806/2011) iakttas.

När en fråga enligt 10 kap. 60 § 3 mom. i tvångsmedelslagen om att skjuta upp eller avstå från underrättelsen om användning av en metod för underrättelseinhämtning behandlas, ska yrkandet framställas av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman.

Den som varit föremål för användningen av en metod för underrättelseinhämtning behöver inte underrättas om detta, om föremålet har varit en statlig aktör.

89 a §

Underrättelse om användning av underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer

Den som varit föremål för underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer underrättas inte om användningen av metoden för underrättelseinhämtning.

En part som med stöd av 17 kap. 13, 14, 16 eller 20 § eller 22 § 2 mom. i rättegångsbalken har skyldighet eller rätt att vägra vittna om information ska underrättas om underrättelseinhämtning som avser datatrafik

Gällande lydelse

Föreslagen lydelse

hos andra än statliga aktörer, om information som omfattas av rätt eller skyldighet att vägra vittna har kommit fram i samband med den underrättelseinhämtning som avser datatrafik. Skyldighet att underrätta personen föreligger emellertid inte, om den information som inhämtats genom underrättelseinhämtning som avser datatrafik har utplånats med stöd av 85 eller 86 §.

(ny)

89 b §

Lämnande och uppskjutande av samt avstående från underrättelse

En underrättelse till en person som avses i 89 § eller 89 a § 2 mom. ska göras skriftligen utan dröjsmål efter det att syftet med användningen av en ovan avsedd metod för underrättelseinhämtning har nåtts. De personer som avses i de bestämmelserna ska dock underrättas om användningen av metoden för underrättelseinhämtning senast ett år efter det att användningen av metoden för underrättelseinhämtning upphörde.

Om den som varit föremål för inhämtande av information inte är identifierad eller personens bostadsort i Finland inte är känd vid utgången av den tidsfrist eller det uppskjutande som avses i denna paragraf, ska personen utan obefogat dröjsmål skriftligen underrättas om användningen av metoden för underrättelseinhämtning så snart personens identitet och bostadsort i Finland har utretts.

Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om den underrättelse som getts till den som varit föremål för underrättelseinhämtning.

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 en underrättelse enligt 89 § 1 mom. och 89 a § 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

Gällande lydelse

Föreslagen lydelse

underrättelseinhämtning, med avseende på landets försvar eller för att garantera den nationella säkerheten eller skydda liv eller hälsa.

Domstolen får besluta att man helt får avstå från underrättelse, om det är nödvändigt med hänsyn till landets försvar eller för att skydda den nationella säkerheten eller liv eller hälsa.

I fråga om handläggning av underrättelseärenden i domstol ska 116 § iakttas.

91 §

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.

91 §

Befogenheter för den som inte arbetar i tjänsteförhållande

En person som tjänstgör med stöd av värnpliktslagen (1438/2007) eller deltar i frivilliga övningar enligt 18 och 19 § i lagen om frivilligt försvar (556/2007) och som har fått tillräcklig utbildning får, för utförandet av ett underrättelseuppdrag, under ledning och övervakning av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman, använda de metoder för underrättelseinhämtning som avses i 4 kap., med undantag för styrd användning av informationskällor, täckoperationer och bevisprovokation genom köp.

En med användningen av metoder för underrättelseinhämtning särskilt förtrogen person som har tagit avsked från en militärunderrättelsemyndighet och som tjänstgör eller deltar i övningar enligt 1 mom. får under ledning och övervakning av en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman använda de metoder för underrättelseinhämtning som avses i 4 kap.

(upphävs)

Gällande lydelse

En reservist som i enlighet med 47 § i lagen om försvarsmakten (55/2007) 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. Reserviläinen saa käyttää tässä pykälässä tarkoitettuja toimivaltuuksia ainoastaan tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa.

En reservist 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.

93 §

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 90 eller 91 §.

94 §

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

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**

Föreslagen lydelse

(upphävs)

93 §

Tjänsteansvar för den som **inte arbetar i tjänsteförhållande**

På en person som utför uppgifter enligt denna lag tillämpas bestämmelserna om straffrättsligt tjänsteansvar.

94 §

Skadeståndsansvar för den som **inte arbetar i tjänsteförhållande**

För en skada som en person som utför uppgifter enligt denna lag har orsakat svarar staten i enlighet med vad som föreskrivs i skadeståndslagen (412/1974).

På skadeståndsansvaret för den som deltar i frivilliga övningar enligt 18 och 19 § i lagen om frivilligt försvar tillämpas bestämmelserna om en värnpliktigs skadeståndsansvar i 4 kap. i skadeståndslagen när personen utför uppgifter enligt denna lag.

9 kap.

Yppandeförbud, skyldigheter och rättigheter som gäller **kommunikationsförmedlare, leverantörer av datacentraltjänster och**

Gällande lydelse

samt användning och erhållande av information

96 §

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.

(ny)

Föreslagen lydelse

dataöverförare samt användning och erhållande av information

96 §

Biståndsskyldighet för kommunikationsförmedlare och leverantörer av datacentraltjänster

En kommunikationsförmedlare och en i 2 § 2 punkten i cybersäkerhetslagen (124/2025) avsedd leverantör av datacentraltjänster ska utan obefogat dröjsmål göra de kopplingar i ett kommunikationsnät eller en datacentraltjänst som behövs för teleavlyssning, teleövervakning och sådan underrättelseinhämtning i hemlandet som avser en statlig aktörs datasystem samt tillhandahålla militärunderrättelsemyndigheterna de uppgifter och redskap samt den personal som behövs för utförande av teleavlyssningen. Detsamma gäller även de situationer där en militärunderrättelsemyndighet genomför teleavlyssning, teleövervakning eller sådan underrättelseinhämtning i ett kommunikationsnät eller en datacentraltjänst i hemlandet som avser en statlig aktörs datasystem med hjälp av tekniska anordningar. Kommunikationsförmedlaren och leverantören av datacentraltjänster ska dessutom ge en med användningen av metoder för underrättelseinhämtning särskilt förtrogen tjänsteman sådana uppgifter som den har i sin besittning och som behövs för teknisk spårning.

Militärunderrättelsemyndigheten, den som utför åtgärden och den biträdande personalen har rätt att för att göra de kopplingar som behövs för teleavlyssning och för sådan underrättelseinhämtning i ett kommunikationsnät i hemlandet som avser en statlig aktörs datasystem få tillträde också till andra utrymmen än de som är i kommunikationsförmedlarens eller leverantörens av informationssamhällets tjänster besittning, dock inte till utrymmen som används för stadigvarande boende. En med användningen av metoder för

Gällande lydelse

Föreslagen lydelse

underrättelseinhämtning särskilt förtrogen tjänsteman beslutar om åtgärden.

97 §

97 §

Dataöverförarens skyldighet att medverka till genomförandet och upprätthållandet av den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter

Dataöverförarens skyldighet att medverka till genomförandet och upprätthållandet av den accesspunkt som underrättelseinhämtning som avser datatrafik förutsätter

Om den accesspunkt som avses i 1 mom. inte kan genomföras med medverkan av dataöverföraren, har Försvarmaktens 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.

Om den accesspunkt som avses i 1 mom. inte kan genomföras med medverkan av dataöverföraren *eller om det är nödvändigt för att skydda underrättelseinhämtning*, har Försvarmaktens underrättelsetjänst rätt att genomföra accesspunkten i den del av ett kommunikationsnät som dataöverföraren administrerar. *Om inte skyddet för underrättelseinhämtning förutsätter något annat*, ska dataöverföraren *om möjligt* vara på plats när den accesspunkt som förutsätts för den underrättelseinhämtning som avser datatrafik genomförs.

99 §

99 §

*Ersättningar till **teleföretag***

*Ersättningar till **kommunikationsförmedlare och leverantörer av datacentraltjänster***

Ett teleföretag har rätt att få ersättning av statens medel för direkta kostnader som orsakats av att företaget i enlighet med 96 § 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 betalning av ersättning.

En kommunikationsförmedlare och leverantör av datacentraltjänster har rätt att så som föreskrivs i 299 § i lagen om tjänster inom elektronisk kommunikation få ersättning av statens medel för direkta kostnader som orsakats av att den i enlighet med 96 § har bistått en militärunderrättelsemyndighet och lämnat uppgifter. Beslut om betalning av ersättning fattas av den militärunderrättelsemyndighet som vidtagit åtgärden.

101 §

101 §

Sökande av ändring i ett ersättningsbeslut

Sökande av ändring i ett ersättningsbeslut

Omprövning av ett beslut om ersättning till ett teleföretag eller en dataöverförare får

Omprövning av ett beslut om ersättning till en kommunikationsförmedlare, leverantör av

Gällande lydelse

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 Transport- och kommunikationsverket tillfälle att bli hört.

104 §

Rätt att få information av privata sammanslutningar

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.

(ny)

111 §

Undersökning av upptagningar

Upptagningar som uppkommit vid användningen av metoder

Föreslagen lydelse

datacentraltjänster eller dataöverförare får begäras. *Bestämmelser om begäran om omprövning finns i förvaltningslagen (434/2003).*

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

(upphävs)

Förvaltningsdomstolen ska ge Transport- och kommunikationsverket tillfälle att bli hört.

104 §

Rätt att få information av privata sammanslutningar

Militärunderrättelsemyndigheterna har i ett enskilt fall på begäran rätt att av *kommunikationsförmedlare och leverantörer av datacentraltjänster* få kontaktuppgifter för teleadresser som inte är upptagna i en offentlig katalog eller information som identifierar en teleadress eller teleterminalutrustning *eller information som behövs för att identifiera en tjänsts användare eller abonnent*, om informationen behövs för utförande av ett underrättelseuppdrag. Militärunderrättelsemyndigheterna har motsvarande rätt att få information om utdelningsadresser av en sammanslutning som bedriver postverksamhet.

Militärunderrättelsemyndigheterna har rätt att få de uppgifter som avses i denna paragraf utan dröjsmål och avgiftsfritt, om inte något annat föreskrivs i lag.

111 §

Undersökning av upptagningar

Upptagningar som uppkommit vid användningen av metoder

Gällande lydelse

underrättelseinhämtning får undersökas endast av domstol och huvudstabens underrättelsechef, en till uppdraget av militärunderrättelsemyndigheterna förordnad och med användningen av metoder för underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman eller av underrättelsetillsynsombudsmannen eller en av denne förordnad tjänsteman. Dessutom får upptagningar på förordnande av huvudstabens underrättelsechef eller enligt anvisning av domstolen också undersökas av en annan än en ovan avsedd tjänsteman vid en militärunderrättelsemyndighet, en sakkunnig eller en annan person som bistår vid inhämtande av information.

Föreslagen lydelse

underrättelseinhämtning får undersökas endast av domstol och huvudstabens underrättelsechef, en till uppdraget av militärunderrättelsemyndigheterna förordnad *tjänsteman eller av* underrättelsetillsynsombudsmannen eller en av denne förordnad tjänsteman. Dessutom får upptagningar på förordnande av *en med användningen av metoder för* underrättelseinhämtning särskilt förtrogen militärjurist eller annan tjänsteman eller enligt anvisning av domstolen också undersökas av en annan än en ovan avsedd tjänsteman vid en militärunderrättelsemyndighet, en sakkunnig eller en annan person som bistår vid inhämtande av information.

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) nya 8 b och 8 c § samt till 36 a §, sådan den lyder i lag 890/2018, ett nytt 3 mom. som följer:

Gällande lydelse

(ny)

Föreslagen lydelse

8 b §

*Inhämtande av information från allmänt
tillgängliga källor*

*Försvarsmakten får för skötseln av sina
uppgifter inhämta och behandla information
från allmänt tillgängliga källor.*

Gällande lydelse

Föreslagen lydelse

Försvarsmakten har rätt att använda tekniska anordningar, metoder eller programvaror för att söka och lagra information som härrör från en i 1 mom. avsedd källa.

Försvarsmakten får vid skyddandet av den informationsinhämtning som avses i 1 mom. använda falska, vilseledande eller förtäckta uppgifter för att hemlighålla uppdraget.

Huvudstaben fattar beslut om de förvaltningsenheter inom Försvarsmakten som ska ha rätt att använda det skydd för informationsinhämtning som avses i 3 mom.

Chefen för en i 4 mom. avsedd förvaltningsenhet beslutar om det skydd för informationsinhämtning som avses i 3 mom.

(ny)

8 c §

Utplåning av uppgifter som inhämtats från allmänt tillgängliga källor

Information som erhållits vid sådan informationsinhämtning som avses i 8 b § ska utplånas utan dröjsmål efter att det har framgått att informationen inte behövs för utförande av Försvarsmaktens uppgifter.

Bestämmelser om behandling av personuppgifter finns i lagen om behandling av personuppgifter inom Försvarsmakten (332/2019).

36 a §

36 a §

Viran haettavaksi julistaminen

Ledigförklarande av tjänster

(ny)

När andra än i 1 eller 2 mom. avsedda tjänster eller tjänsteförhållanden tillsätts genom ett ansökningsförfarande, kan Försvarsmakten låta bli att meddela dem som sökt tjänsten eller tjänsteförhållandet namnen på de andra sökandena och namnet på den som har utnämnts, om uppgiftens art nödvändigt kräver det. Sökandena ska dock underrättas om att tjänsten eller tjänsteförhållandet har tillsatts, och i utnämningsbeslutet ska nämnas den tjänst eller det tjänsteförhållande som tillsätts,

Gällande lydelse

Föreslagen lydelse

vilken myndighet som har fattat beslutet samt datum för utnämningen.

Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 17 kap. 7 § i strafflagen

I enlighet med riksdagens beslut

ändras i strafflagen (39/1889) 17 kap. 7 § 2 mom., sådant det lyder i lag 650/2004, som följer:

Gällande lydelse

Föreslagen lydelse

7 §

7 §

Riksgränsbrott

Riksgränsbrott

För riksgränsbrott döms inte en utlänning som med anledning av en sådan gärning som avses i 1 mom. avvisas eller utvisas och inte heller en utlänning som på grund av flyktingskap ansöker om asyl eller uppehållstillstånd i Finland. För riksgränsbrott döms inte heller en utlänning som har begått ett brott enligt 1 mom. till följd av att han eller hon har varit föremål för människohandel enligt 25 kap. 3 eller 3 a §.

För riksgränsbrott döms inte en utlänning som med anledning av en sådan gärning som avses i 1 mom. avvisas eller utvisas och inte heller en utlänning som på grund av flyktingskap ansöker om asyl eller uppehållstillstånd i Finland. För riksgränsbrott döms inte heller en utlänning som har begått ett brott enligt 1 mom. till följd av att han eller hon har varit föremål för människohandel enligt 25 kap. 3 eller 3 a § eller som har begått en i 1 mom. avsedd gärning på grundval av 78 a § 3 mom. i lagen om militär underrättelseverksamhet.

Denna lag träder i kraft den 20 .

4.

Lag

om ändring av 71 d § i lagen om Finansinspektionen

I enlighet med riksdagens beslut
ändras i lagen om Finansinspektionen (878/2008) 71 d §, sådan den lyder i lag 276/2025, som följer:

Gällande lydelse

71 d §

Rätt att lämna ut uppgifter till skyddspolisen

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet har Finansinspektionen rätt att *utan hinder av sekretessbestämmelserna* på begäran lämna ut information till skyddspolisen om informationen är nödvändig för förebyggande av brott som hör till skyddspolisens verksamhetsområde och för skyddande av den nationella säkerheten mot verksamhet som utgör ett allvarligt hot mot den.

Finansinspektionen har rätt att utan hinder av sekretessbestämmelserna på eget initiativ till skyddspolisen lämna ut information som Finansinspektionen har i sin besittning gällande penningtvätt eller finansiering av terrorism, kringgående av sanktionsbestämmelser eller andra ovanliga transaktioner genom vilka medel överförs till tredjeländer och åtgärderna misstänks äventyra den nationella säkerheten, om informationen är behövlig för förebyggande av brott som hör till skyddspolisens verksamhetsområde och för skyddande av den nationella säkerheten mot verksamhet som allvarligt hotar den.

På utlämnande av den information som avses i 1 och 2 mom. tillämpas det som föreskrivs i 71 § 5 mom.

Föreslagen lydelse

71 d §

Rätt att lämna ut uppgifter till skyddspolisen och militärunderrättelsemyndigheterna

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet har Finansinspektionen rätt att *trots sekretessbestämmelserna* på begäran lämna ut information till skyddspolisen, om informationen är nödvändig för förebyggande av brott som hör till skyddspolisens verksamhetsområde och för skyddande av den nationella säkerheten mot verksamhet som utgör ett allvarligt hot mot den, *samt till en militärunderrättelsemyndighet, om informationen är nödvändig med tanke på militärunderrättelsemyndighetens underrättelseuppdrag.*

Finansinspektionen har rätt att *trots sekretessbestämmelserna* på eget initiativ till skyddspolisen *eller militärunderrättelsemyndigheten* lämna ut information som Finansinspektionen har i sin besittning gällande penningtvätt eller finansiering av terrorism, kringgående av sanktionsbestämmelser eller andra ovanliga transaktioner genom vilka medel överförs till tredjeländer, *om* åtgärderna misstänks äventyra den nationella säkerheten *och* om informationen är behövlig för förebyggande av brott som hör till skyddspolisens verksamhetsområde och för skyddande av den nationella säkerheten mot verksamhet som allvarligt hotar den *eller om informationen är behövlig med tanke på militärunderrättelsemyndighetens underrättelseuppdrag.*

På utlämnande av den information som avses i 1 och 2 mom. tillämpas det som föreskrivs i 71 § 5 mom.

Denna lag träder i kraft den 20 .

5.

Lag

om ändring av 6 § i lagen om Enheten för utredning av grå ekonomi

I enlighet med riksdagens beslut
ändras i lagen om Enheten för utredning av grå ekonomi (1207/2010) 6 § 1 mom. 40 punkten, sådan den lyder i lag 24/2026, samt
fogas till 6 § 1 mom., sådant det lyder i lagarna 308/2016, 858/2016, 1159/2016, 1413/2016, 1419/2016, 324/2017, 454/2017, 1112/2017, 404/2018, 414/2018, 722/2019, 1399/2019, 624/2020, 488/2021, 690/2021, 1134/2021, 495/2022, 713/2022, 1119/2022, 1327/2022, 1340/2022, 1355/2022, 743/2023, 190/2024, 940/2024, 260/2025, 277/2025 och 24/2026, en ny 41 punkt som följer:

Gällande lydelse

Föreslagen lydelse

6 §

6 §

Syftet med fullgöranderapporter

Syftet med fullgöranderapporter

Fullgöranderapporter utarbetas till stöd för

Fullgöranderapporter utarbetas till stöd för

40) utredning av tillförlitlighet och lämplighet som det föreskrivs om i 10 § i penningsspeklagen (10/2026).
(ny)

40) utredning av tillförlitlighet och lämplighet som det föreskrivs om i 10 § i penningsspeklagen (10/2026),

41) militär underrättelseinhämtning som avses i lagen om militär underrättelseverksamhet (590/2019).

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av 92 b § i inkomstskattelagen

I enlighet med riksdagens beslut
ändras i inkomstskattelagen (1535/1992) 92 b § 3 punkten, sådan den lyder i lag 404/2025, som följer:

Gällande lydelse

Föreslagen lydelse

92 b §

92 b §

*Vittnesarvode, belöning för tips och arvode
som betalas för användning av
informationskälla*

*Vittnesarvode, belöning för tips och arvode
som betalas för användning av
informationskälla*

Skattepliktig inkomst är inte

Skattepliktig inkomst är inte

3) arvode som en myndighet betalar en i lagen om militär underrättelseverksamhet (590/2019) och i polislagen (872/2011) avsedd informationskälla för inhämtande av uppgifter som är av betydelse för skötseln av ett underrättelseuppdrag samt en i lagen om brottsbekämpning inom Gränsbevakningsväsendet (108/2018) avsedd informationskälla för inhämtande av uppgifter som är av betydelse för skötseln av uppdrag som hänför sig till upprätthållandet av gränssäkerheten.

3) arvode som en myndighet betalar en i lagen om militär underrättelseverksamhet (590/2019) och i polislagen (872/2011) avsedd informationskälla för inhämtande av för skötseln av ett underrättelseuppdrag betydelsefulla uppgifter eller för biträdande av en underrättelsemyndighet och en i lagen om brottsbekämpning inom Gränsbevakningsväsendet (108/2018) avsedd informationskälla för inhämtande av uppgifter som är av betydelse för skötseln av uppdrag som hänför sig till upprätthållandet av gränssäkerheten.

Denna lag träder i kraft den 20 .

7.

Lag

om ändring av gränsbevakningslagen

I enlighet med riksdagens beslut ändras i gränsbevakningslagen (578/2005) 3 § 3 mom., sådant det lyder i lag 749/2014, och fogas till lagen en ny 25 a § som följer:

Gällande lydelse

Föreslagen lydelse

3 §

3 §

Gränsbevakningsväsendets uppgifter

Gränsbevakningsväsendets uppgifter

Gällande lydelse

Gränsbevakningsväsendet utför polis- och tulluppgifter, efterspanings- och räddningsuppgifter och prehospital akutsjukvård samt deltar i det militära försvaret. Bestämmelser om gränsbevakningsväsendets uppgifter inom området för sjöräddningstjänsten finns i sjöräddningslagen.

(ny)

Föreslagen lydelse

Gränsbevakningsväsendet utför polis- och tulluppgifter, efterspanings- och räddningsuppgifter och prehospital akutsjukvård samt deltar i det militära försvaret och i militär underrättelseinhämtning. Bestämmelser om gränsbevakningsväsendets uppgifter inom området för sjöräddningstjänsten finns i sjöräddningslagen.

25 a §

Gränsbevakningsväsendets deltagande i militär underrättelseinhämtning

Gränsbevakningsväsendet deltar på en underrättelsemyndighets begäran i militär underrättelseinhämtning genom att inhämta information och genom att vidta åtgärder till stöd för militärunderrättelsemyndigheternas underrättelseuppdrag.

Bestämmelser om gränsbevakningsväsendets befogenheter vid deltagande i militär underrättelseinhämtning finns i lagen om militär underrättelseverksamhet (590/2019).

Denna lag träder i kraft den 20 .

8.

Lag

om ändring av 32 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet

I enlighet med riksdagens beslut fogas till 32 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019), sådan paragrafen lyder i lag 430/2024, ett nytt 2 mom. som följer:

Gällande lydelse

32 §

Föreslagen lydelse

32 §

Gällande lydelse

Föreslagen lydelse

*Utlämnande av personuppgifter till en annan
behörig myndighet som avses i
dataskyddslagen avseende brottmål*

*Utlämnande av personuppgifter till en annan
behörig myndighet som avses i
dataskyddslagen avseende brottmål*

(ny)

Gränsbevakningsväsendet får trots sekretessbestämmelserna lämna ut sådana uppgifter som avses i 15 b § till Försvarsmakten för skötseln av de uppgifter som anges i lagen om militär underrättelseverksamhet (590/2019).

Denna lag träder i kraft den 20 .

9.

Lag

om ändring av lagen om behandling av personuppgifter inom Försvarsmakten

I enlighet med riksdagens beslut
fogas till lagen om behandling av personuppgifter inom Försvarsmakten (332/2019) en ny 37 a § som följer:

Gällande lydelse

(ny)

Föreslagen lydelse

37 a §

*Militärunderrättelsemyndighetens rätt att
upprätthålla sitt personregister*

Om en personuppgiftsansvarig enligt någon annan lag har rätt att ur sitt personregister lämna ut personuppgifter till Försvarsmakten genom en teknisk anslutning eller som en datamängd trots sekretessbestämmelserna, får militärunderrättelsemyndigheten för att upprätthålla sitt informationssystem jämföra uppgifterna i personregistret i fråga med innehållet i sina registrerade personuppgifter. Onödiga uppgifter ska raderas utan dröjsmål efter det att jämförelsen har gjorts. Onödiga personuppgifter får inte registreras.

Om det föreskrivs att den nationella säkerheten eller landets försvar är det ursprungliga ändamålet med behandlingen av uppgifterna eller att landets försvar eller den

Gällande lydelse

Föreslagen lydelse

nationella säkerheten är ett annat ändamål än det ursprungliga, har militärunderrättelsemyndigheten dessutom trots sekretessbestämmelserna rätt att i sitt informationssystem jämföra en datamängd insamlad från ett annat informationssystem, om förfarandet är nödvändigt för att göra behandlingen av uppgifter möjlig i ett informationssystem med hög informationssäkerhetsnivå. Datamängden ska förstöras utan dröjsmål efter det att behovet av jämförelse har upphört. De uppgifter som insamlas för jämförelsen ska hållas åtskilda från övriga uppgifter som militärunderrättelsemyndigheten behandlar.

Denna lag träder i kraft den 20 .