Försvarsministeriet, Finland
Mars 2015

RIKTLINJER FÖR EN FINSK UNDERRÄTTELSELAGSTIFTNING

Arbetsgruppsbetänkande

FÖRSVARSMINISTERIET **PRESENTATIONSBLAD**

14.1.2015

Författare

Arbetsgruppen för en informationsanskaffningslag
Hanna Nordström (ordförande)
Katriina Laitinen (vice ordförande)
Mika Lundelin (arbetsgruppsmedlem)
Jenni Herrala (sekreterare)
Jan Sjöblom (sekreterare)
Kosti Honkanen (sekreterare)
Minnamaria Nurminen (sekreterare)

Typ av publikation	arbetsgruppsbetänkande
Uppdragsgivare	försvarsministeriet
Datum då organet tillsattes	13.12.2013

Publikation (även den finska titeln)

Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintatyöryhmän mietintö.
Riktlinjer för en finsk underrättelselagstiftning. Betänkande av arbetsgruppen för en informationsanskaffningslag

Publikationen är tillgänglig på internet på adressen **www.defmin.fi**

Sammandrag

I detta betänkande bedöms behoven att utveckla en lagstiftning om underrättelse.

Informationsinhämtning i datanätsomgivningen för att identifiera allvarliga hot, vilken utförs av de myndigheter som svarar för den nationella säkerheten, är till sin art underrättelse. Finland har ingen lagstiftning om underrättelse. Arbetsgruppen föreslår att det ska övervägas om regeringen kan inleda nödvändiga åtgärder för att skapa en författningsgrund för underrättelse.

Syftet med underrättelsen är att skaffa den information om allvarliga internationella hot som är nödvändig med tanke på den nationella säkerheten. Hoten kan vara militära eller civila. Genom underrättelse säkerställs att statens högsta lednings beslutsfattande grundar sig på korrekt, aktuell och tillförlitlig information samt möjliggörs att behöriga myndigheter kan vidta åtgärder för att avvärja hoten.

För de militära och civila myndigheter som svarar för den nationella säkerheten bör övervägas gränsöverskridande befogenheter att bedriva underrättelse som riktas mot datatrafiken för att förändringar i säkerhetsomgivningen ska kunna bemötas. Det tekniska genomförandet av datatrafikspaning vore det ändamålsenligt att koncentrera till en myndighet.

Det bör övervägas om försvarsmakten och Skyddspolisen kan få befogenheter för utlandsunderrättelse för att skaffa information om personer och datasystem. Eftersom det med underrättelse utomlands sammanhänger utrikespolitiskt sensitiva element, bör vid beslutsfattandet om sådan beaktas de riktlinjer som statens högsta ledning har dragit upp. Styr- och ansvarsförhållandena bör bedömas i samband med den eventuella fortsatta beredningen.

Till datatrafikspaningen bör ett oavhängigt tillståndsförfarande fogas. För datatrafikspaning och underrättelse utomlands bör ett oavhängigt tillsynssystem skapas.

När beredningen av en lagstiftning om datatrafikspaning övervägs, bör sekretesskyddet för konfidentiella meddelanden, som har tryggats för var och en i form av en grundläggande fri- och rättighet och en mänsklig rättighet, beaktas. Det verkar som om det inte vore möjligt att stifta en lag om datatrafikspaning som ska bedrivas i underrättelsesyfte utan att grundlagen ändras, eventuellt med undantag för sådan spaning som enbart riktar sig mot en främmande stats datatrafik.

Försvarsministeriet, Finland
Mars 2015

Försvarsministeriet, Finland
Mars 2015

Till försvarsministeriet

Försvarsministeriet tillsatte den 13 december 2013 en arbetsgrupp för att utveckla lagstiftning för att förbättra säkerhetsmyndigheternas förmåga att inhämta information om hot i cyberomgivningen. Arbetsgruppen skulle få sitt arbete klart senast den 30 juni 2014.

Försvarsministeriet förlängde den 27 maj 2014 arbetsgruppens mandatperiod till den 31 december 2014.

Arbetsgruppen hade till uppgift att bedöma behovet att utveckla den finska lagstiftningen så att man i Finland kan sörja för den nationella säkerheten för att avvärja de hot som förekommer i datanäten.

Vidare hade arbetsgruppen till uppgift att sammanställa synpunkter på de hot som via datanäten riktas mot Finlands säkerhet och på dessa hots konsekvenser för Finlands säkerhet och konkurrenskraft, reda ut nuläget och utvecklingsförslagen gällande säkerhetsmyndigheternas informationsinhämtning, till behövliga delar granska den lagstiftning som gäller säkerhetsmyndigheternas informationsinhämtning i vissa andra länder, göra en konsekvensbedömning av de olika utvecklingsalternativen och utifrån det som retts ut ge förslag på hur lagstiftningen kunde utvecklas samt en framställning om de åtgärder som verkställigheten av förslagen förutsätter.

Enligt uppdraget kunde arbetsgruppens betänkande göras i form av en regeringsproposition eller också kunde i betänkandet inbegripas förslag på hur separata lagstiftningsprojekt kunde inledas.

Till ordförande för arbetsgruppen förordnades regeringsråd, såsom lagstiftningsdirektör Hanna Nordström från försvarsministeriet och till vice ordförande regeringsrådet, senare polisavdelningens lagstiftningsdirektör, Katriina Laitinen från inrikesministeriet.

Till medlemmar i arbetsgruppen kallades juridiska rådgivaren Minna Hulkkonen från republikens presidents kansli, enhetschef Mikko Kinnunen från utrikesministeriet, lagstiftningsdirektör Sami Manninen från justitieministeriet, polisinspektör Jari Pajunen från inrikesministeriet, enhetschef Timo Junttila och regeringssekreterare Pia Palojärvi från försvarsministeriet (till den 4 juni 2014), budgetrådet Petri Syrjänen från finansministeriet, enhetschef, lagstiftningsrådet Kirsi Miettinen från kommunikationsministeriet (till den 24 oktober 2014), regeringsrådet, senare personal- och förvaltningsdirektör Kari Mäkinen från arbets- och näringsministeriet, polisdirektör Tomi Vuori från Polisstyrelsen, sektorledare Mika Lundelin från Huvudstaben (från den 4 juni 2014) och kommunikationsrådet, enhetschef Päivi Antikainen från kommunikationsministeriet (från den 24 oktober 2014).

Till ständiga sakkunniga kallade arbetsgruppen rättschef Päivi Kaukoranta från utrikesministeriet, lagstiftningsrådet Sami Kivivasara från finansministeriet (till den 4 juni 2014), lagstiftningsrådet Hannele Kerola från finansministeriet (från den 4 juni 2014), polisrådet Antti Pelttari och biträdande chef Petri Knape från Skyddspolisen, underrättelsechef Harri Ohra-aho från huvudstaben,

överste Martti J. Kari från försvarsmakten och konsultativ tjänsteman Laura Tarhonen från kommunikationsministeriet (från den 10 september 2014).

I arbetsgruppens arbete har systemsakkunnig Sari Kajantie från Skyddspolisen och ingenjörskapten Jouni Flyktman från försvarsmakten deltagit i egenskap av tekniska sakkunniga.

Sekreterare för arbetsgruppen har varit regeringssekreterare Jenni Herrala, äldre regeringssekreterare Minnamaria Nurminen och föredragande Kosti Honkanen (från den 4 juni 2014) från försvarsministeriet, överinspektör Jan Sjöblom från Skyddspolisen och sektorledare Mika Lundelin från huvudstaben (till den 4 juni 2014). Arbetsgruppen tog sig namnet arbetsgruppen för en informationsinhämtningslag. Arbetsgruppen har hållit 45 möten.

Under arbetets gång har arbetsgruppen hört följande personer:

lägesbildskoordinator, enhetschef Jarkko Korhonen, statsrådets kansli
statsrådets säkerhetsdirektör Timo Härkönen, statsrådets kansli
dataadministrationsdirektör Ari Uusikartano, utrikesministeriet
specialsakkunnig Kimmo Janhunen, finansministeriet

direktören för EU:s underrättelseanalyscentrum Ilkka Salmi
EU:s militärunderrättelsechef Georgij Alafuzoff

dataombudsman Reijo Aarnio
professorn i juridik Veli-Pekka Viljanen, Åbo universitet

beredskapschef ICT Christian Fjäder, Försörjningsberedskapscentralen
direktör Kirsi Karlamaa, Kommunikationsverket
säkerhetsregleringsgruppens chef Jarkko Saarimäki, Cybersäkerhetscentret
informationssäkerhetsexpert Tomi Hasu, Cybersäkerhetscentret
chefen för Centralkriminalpolisen, polisrådet Robin Lardot
kriminalkommissarie Timo Piiroinen, Centralkriminalpolisen
systemsakkunnig Pasi Paunu, Skyddspolisen

Nordic Policy Counsel David Mothander, Google
förvaltnings- och säkerhetsdirektör Vesa Vuoti DNA Oyj
Head of Special Network Security Krister Kaipio, TeliaSonera Finland Oyj
säkerhetsdirektör Jaakko Wallenius, Elisa Oyj
Platform Strategy Manager Pasi Mäkinen, Microsoft Oy
Vice President Kaisa Olkkonen, Nokia Government Relations
Head of Security Technologies Gabriel Waller, Nokia Solutions and Networks
forskningsdirektör Mikko Hyppönen, F-Secure Oyj
teknologiedirektör Kimmo Kasslin, F-Secure Oyj
smf-direktör Jyrki Hollmén, Finlands näringsliv
Associate Partner Vesa Weissmann, Gearshift Group Oy

Dessutom har arbetsgruppen konfidentiellt hört två utländska sakkunniga om effektiviteten i och nödvändigheten av underrättelseinhämtning i datakommunikationen.

Arbetsgruppen ordnade den 12 mars 2014 ett evenemang för redaktörer, vid vilket bakgrundsinformation gavs om detta projekt, och en allmän hearing för näringslivets representanter den 29 april 2014 och en för medborgarorganisationer och andra intressegrupper den 6 maj 2014.

Försvarsministeriet har på uppdrag av arbetsgruppen beställt en undersökning, där de utländska investeringarna på IT-sektorn i Finland och Sverige under åren 2008–2013 samt de eventuella konsekvenserna av Sveriges signalspaningslag på investeringarna i Sverige reddes ut.

När man bedömde eventuella behov av reglering av informationsinhämtningen i datanät visade det sig att utvecklandet av lagstiftningen borde granskas mera vidsträckt med tanke på säkerhetsmyndigheternas underrättelseuppgift. När det gäller att förbättra säkerhetsmyndigheternas förmåga att inhämta information är det inte i första hand fråga om att förbättra dataskyddet, utan om att ge myndigheterna bättre möjligheter att förhindra allvarliga dåd som hotar den nationella säkerheten. Arbetsgruppen har inte skrivit sitt betänkande i form av en regeringsproposition. I arbetsgruppens betänkande bedöms nuläget i fråga om säkerhetsmyndigheternas inhämtning av information och ges utvecklingsförslag till uppgifter och nya befogenheter som gäller underrättelse.

Till arbetsgruppens betänkande har lämnats en avvikande åsikt och två yttranden, och dessa ingår som bilagor till betänkandet.

Efter att ha fått sitt arbete klart överlåter arbetsgruppen med högaktning sitt betänkande till försvarsministeriet.

Helsingfors den 14 januari 2015

Försvarsministeriet, Finland
Mars 2015

	Hanna Nordström	Katriina Laitinen
Päivi Antikainen	Minna Hulkkonen	Timo Junttila
Mikko Kinnunen	Mika Lundelin	Sami Manninen
Kari Mäkinen	Jari Pajunen	Petri Syrjänen
		Tomi Vuori
Martti J. Kari	Päivi Kaukoranta	Hannele Kerola
Petri Knape	Harri Ohra-aho	Antti Pelttari
		Laura Tarhonen
	Jenni Herrala	Kosti Honkanen
	Minnamaria Nurminen	Jan Sjöblom

INNEHÅLL

1 INLEDNING

1.1 Bakgrund

Den allmänna utvecklingen gällande internationalisering och teknifiering är viktig och nödvändig. Som en följd av den har Finlands säkerhetspolitiska omgivning förändrats i betydande grad och blivit mera komplicerad under de senaste åren. De hot som riktar sig mot den inre och den yttre säkerheten överlappar varandra allt mera. De allvarligaste hoten mot den nationella säkerheten är så gott som utan undantag av internationellt ursprung eller åtminstone har de kopplingar utanför vårt land. Även med finska intressen utomlands – inklusive de krishanteringsinsatser som Finland deltar i – är mera och allvarligare hot än tidigare förknippade. Det har blivit svårare att identifiera de statliga och icke-statliga parter som står bakom hoten och att förutse deras aktioner. Den datatekniska utvecklingen har gett också små stater och icke-statliga aktörer en möjlighet att agera effektivt. Den teknologiska utvecklingen har gjort det möjligt att genomföra dåd som äventyrar den nationella säkerheten med kortare förberedelsetid och med allvarligare följder. Attacker som utförs i datanät kan användas för politisk och ekonomisk påtryckning och i en allvarlig kris som ett påverkansmedel utöver traditionella militära maktmedel.
Hotens internationella karaktär innebär att de parter som står bakom dem har bildat nätverk inom flera länders territorier. De som är delaktiga kommunicerar över statsgränserna. Den snabba utvecklingen inom kommunikationsteknologin har effektiverat och underlättat de gränsöverskridande kontakterna och nätverkandet mellan de parter som utgör ett hot för Finland samt påskyndat internationaliseringen av hoten. Utöver aktörerna på den civila sidan stöder sig också ledningen av moderna väpnade styrkor mera än tidigare på den allmänna teleinfrastrukturen. Till följd av datateknikens snabba utveckling och lägre kostnader tar väpnade styrkor i stor utsträckning i bruk sådana lednings- och kommunikationssystem som har planerats för civila behov.

1.2 Något om föremålet för arbetet

I det brev genom vilket arbetsgruppen tillsattes och som är daterat den 13 december 2013 gavs arbetsgruppen till uppgift att utveckla den finska lagstiftningen särskilt vad gäller regleringen av säkerhetsmyndigheternas inhämtande av information. Enligt brevet om tillsättande var målet att man skulle sörja bättre för den nationella säkerheten för att avvärja i synnerhet de hot som förekommer i datanäten.

Cybersäkerheten togs upp redan i en säkerhetsstrategi för samhället från år 2010 (statsrådets principbeslut av den 16 december 2010). Cyberhoten identifierades som ett möjligt hot, och intrång i datasystem konstaterades under vissa omständigheter till och med kunna uppfylla kännetecknen på användning av militära maktmedel. I strategin för cybersäkerheten i Fin-

land från år 2013 (statsrådets principbeslut av den 24 januari 2013) stakades en vision ut enligt vilken Finland år 2016 är en global föregångare när det gäller att förbereda sig på cyberhot och hantera störningssituationer förorsakade av dessa.

Vid utvecklandet av säkerhetsmyndigheternas förmåga att inhämta information är det i detta betänkande inte i första hand frågan om att förbättra dataskyddet. Det är inte heller frågan om att avvärja sådan nätbrottslighet som ska anses sedvanlig utan det är frågan om att upptäcka och identifiera allvarliga hot som riktar sig mot den nationella säkerheten och om att göra det möjligt att avvärja sådana hot. Målet är att förbättra den högsta statsledningens samt säkerhetsmyndigheternas tillgång på information om sådana hot samt om utvecklingen i den finska säkerhetspolitiska omgivningen. För den högsta statsledningen måste man kunna producera opartisk och tillförlitlig information i tillräckligt god tid för beslutsfattandet så att man med hjälp av denna information kan påverka och förbereda sig på de hot, risker och möjligheter som förekommer i den säkerhetspolitiska omgivningen. Det är viktigt för hela samhället och för att näringslivet ska fungera att den nationella säkerheten kan garanteras genom att underrättelseinformation inhämtas. Därför måste nuläget i fråga om säkerhetsmyndigheternas informationsinhämtning granskas och utvecklingsförslag som anknyter till detta kartläggas.

Myndigheterna på inrikesministeriets förvaltningsområde svarar för att hot av civil art, som riktar sig mot den nationella säkerheten, avvärjs här i Finland. Skyddspolisen är en riksomfattande polisenhet, som har till uppgift att avvärja sådana projekt och brott som kan äventyra stats- och samhällsordningen eller rikets inre och yttre säkerhet samt utreda sådana brott. Skyddspolisen ska också upprätthålla och utveckla den allmänna beredskapen att förhindra verksamhet som äventyrar rikets säkerhet. Skyddspolisen utför inom sitt verksamhetsområde fortgående säkerhetsunderrättelse i enlighet med sin uppgift samt upprätthåller den nationella och internationella lägesbild över statens säkerhetspolitiska omgivning som uppkommer på detta sätt samt rapporterar om dessa till statsledningen och säkerhetsmyndigheterna.

Polisens befogenheter att inhämta information har till den del de ingår i tvångsmedels- och polislagen nyligen förnyats. Däremot har inga särskilda befogenheter föreskrivits för Skyddspolisen i fråga om sådan informationsinhämtning som hänför sig till underrättelse utan dess befogenheter att inhämta information grundar sig på de allmänna lagar som gäller polisen. Användningen av befogenheterna till informationsinhämtning är bunden vid förebyggandet och avslöjandet av ett brott. I betänkandet framhävs utvecklandet av lagstiftningen i enlighet med uppdraget särskilt till den del som gäller normeringen i fråga om Skyddspolisens informationsinhämtning.

Försvarsmakten, som hör till försvarsministeriets förvaltningsområde, svarar för det militära försvaret av Finland. Förvaltningsområdets behov att inhämta information hänför sig till sammanställandet och upprätthållandet av en militärstrategisk lägesbild samt till säkerheten i de internationella uppdragen. Försvarsmaktens spanings- och övervakningssystem följer utvecklingen i den finska säkerhetspolitiska omgivningen, fastslår ändringar i omgivningen

och producerar information om det rådande läget. Systemet ger statsledningen en förvarning om hur militära hot utvecklas, vilket gör det möjligt för statsledningen att fatta beslut i rätt tid och att leda samhällets vitala funktioner. Det finns inga uttryckliga bestämmelser i lag om försvarsmaktens inhämtning av information i underrättelsehänseende, dvs. om militärunderrättelse. Enligt förarbetet till lagen om försvarsmakten (551/2007) är produktion av information en del av försvarsmaktens uppgifter men några egentliga befogenheter ingår inte i lagen.

I Finland har ingen lag stiftats om vad som eftersträvas med underrättelseverksamheten eller hurdan underrättelseverksamhet som kan bedrivas. Säkerhetsmyndigheternas befogenheter gällande informationsinhämtning är bristfälliga i förhållande till verksamhetens samhälleliga betydelse samt i jämförelse med andra länder. Situationen är otillfredsställande, när man beaktar att betydande ändringar har skett i Finlands internationella säkerhetspolitiska omgivning under de senaste åren.

I detta betänkande beskrivs den föränderliga säkerhetspolitiska omgivningen och nuläget i fråga om den informationsinhämtning som hänför sig till den nationella säkerheten. I betänkandet beskrivs vidare lagstiftningen i jämförbara länder, bedöms behovet av en finsk underrättelselagstiftning, bedöms konsekvenserna av utvecklingsförslagen samt föreslås riktlinjer för hur lagstiftningen kan utvecklas.

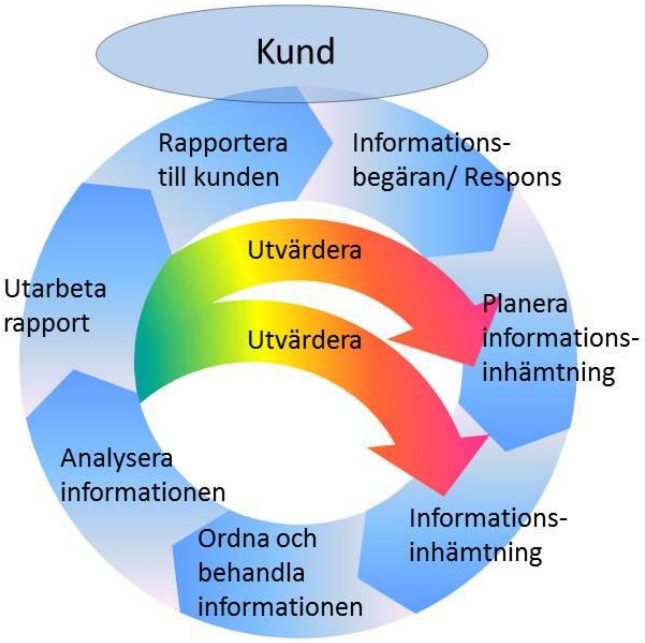
1.3 Begrepp

Eftersom ingen lag om underrättelse har stiftats i Finland, är den begreppsapparat som beskriver underrättelse och dess olika delområden icke-etablerad och mångtydig. För att kunna gestalta underrättelse och dess närliggande fenomen samt kopplingarna till och skillnaderna mellan dem krävs kännedom om den centrala terminologin.

Underrättelsens allmänna begrepp

Underrättelse: Informationsinhämtning som inriktas på offentliga och icke-offentliga källor och vars syfte är att kartlägga och öka förståelsen för olika hot, risker, möjligheter och förändringar såväl inom landet som utanför dess gränser. Syftet med underrättelseverksamhet är att producera information i ett tidigt skede, vilket gör det möjligt att påverka och förbereda sig på hot, risker, möjligheter och ändringar. I underrättelse ingår analysering av informationen, med hjälp av vilken man försöker strukturera, minska och från fall till fall också utnyttja olika slag av osäkerhetsfaktorer i den säkerhetspolitiska omgivningen.

Underrättelsecykel: Underrättelsecykeln beskriver förhållandet mellan kunden och den som skaffar informationen samt processerna för informationsinhämtning, rapportering och analys och växelverkan mellan dessa. En beskrivning av cykeln finns nedan:



Militärunderrättelse: Underrättelse som utförs av militärmyndigheter och genom vilken produceras strategisk och operativ information om och bedömningar av verksamhetsmiljön som stöd för den högsta statsledningens och försvarsmaktens lednings beslutsfattande. Militärunderrättelsen svarar för att en strategisk, operativ och taktisk förvarning ges, utgör stöd för målanvisning och för den information om plats och förhållanden som försvarsmakten behöver. Förvarningen gör det möjligt att vidta motåtgärder mot ett hot.

Civilunderrättelse: Underrättelse som utförs av en civil myndighet genom vilken produceras information som stöd för den högsta statsledningens beslutsfattande och den egna operativa verksamheten i fråga om andra teman än de som hänför sig till området för det militära försvaret.

Säkerhetsunderrättelse: Underrättelse där syftet är att upptäcka, identifiera, förstå och avvärja hot som riktas mot statens inre eller yttre säkerhet. Säkerhetsunderrättelsens informationsinhämtning riktar sig mot en vidsträckt omgivning och den är inte på samma sätt bunden vid ett brott som kriminalunderrättelsen.

Kriminalunderrättelse: Underrättelse som utförs av en lagövervakningsmyndighet och där syftet är att skaffa information om brottslingar, brott och de förhållanden där ett brott har begåtts, vilken är av betydelse för att ett brott ska kunna förhindras, avslöjas eller utredas.

Centrala former av underrättelse

Underrättelseverksamhet med hjälp av öppna källor (OSINT, Open Source Intelligence): Informationsinhämtning som inriktar sig på offentliga källor såsom litteratur, kartor, tidningar och offentliga dokument samt Internet-webbplatser.

Signalspaning (eller i vidare bemärkelse signalunderrättelsetjänst) (SIGINT, Signals Intelligence): Spaning som utförs av en militär- eller civilmyndighet och som inriktas på elektroniska signaler. Signalspaningens viktigaste underbegrepp som har etablerat sig internationellt är:

- kommunikationsspaning (COMINT, Communications Intelligence) med vilken avses elektronisk spaning som inriktar sig på elektronisk kommunikation
- teknisk signalspaning (ELINT, Electronic Intelligence) med vilken avses elektronisk spaning och övervakning som inriktar sig på sensor- och navigeringssignaler och andra signaler som tekniska anordningar avger. Teknisk signalspaning inriktas inte på kommunikationen mellan människor.

Personbaserad underrättelseinhämtning (HUMINT, Human Intelligence): Underrättelseinhämtning genom personkontakt eller genom personlig iakttagelse av en person eller ett annat objekt. Personbaserad underrättelseinhämtning kan också idkas genom ett datanät.

Specialbegrepp som används i betänkandet

För betänkandet har begreppen datatrafikspaning, spaning i utländska datasystem och personbaserad underrättelseinhämtning utomlands bildats.

Med datatrafikspaning avses spaning som inriktar sig på den datatrafik som rör sig i de datakommunikationstrådar som överskrider den finska gränsen. Datatrafikspaningen är signalspaning. Av signalspaningens underarter kan den inbegripa både kommunikationsspaning och teknisk signalspaning.

Med spaning i utländska datasystem avses spaning som görs med datatekniska metoder och som inriktas på uppgifter som behandlas i datasystem utomlands.

Med personbaserad underrättelseinhämtning utomlands avses underrättelseinhämtning utomlands genom personkontakt eller genom personligt iakttagande av en person eller ett annat objekt.

I spaning i utländska datasystem och personbaserad underrättelseinhämtning utomlands är det fråga om verksamhet utomlands, vilket gör att om dem kan användas den gemensamma benämningen underrättelse utomlands. Den gemensamma nämnaren för datatrafikspaning

och spaning i utländska datasystem är igen det att de båda sker i datanät. Således kan om dessa användas det gemensamma övre begreppet datanätsspaning.

2 DEN FÖRÄNDERLIGA SÄKERHETSPOLITISKA OMGIVNINGEN

2.1 En bred säkerhetsuppfattning

Statsrådet gav den 20 december 2012 riksdagen en redogörelse över Finlands säkerhets- och försvarspolitik 2012 (nedan redogörelsen 2012). Redogörelsen 2012 granskar en period som sträcker sig ända till 2020-talet och den utgör grund för styrningen av den finska politiken för att landets intressen och målsättningar ska kunna främjas. I redogörelsen 2012 behandlas accentuerat de utvecklingstrender som finns i den internationella omgivningen samt vilken betydelse globaliseringen av säkerhetsfrågorna har på Finlands säkerhet.

Enligt redogörelsen 2012 är de nätverksbaserade moderna samhällsstrukturerna allt mera beroende av den kritiska infrastrukturen till vilken hör bl.a. trafik, kommunikation och energiförsörjning. Utöver detta betonas att det ökande ömsesidiga beroendet och den alltmera teknifierade omgivningen också har medfört en ny sårbarhet hos samhällena. Nästan alla samhällets kritiska funktioner och tjänster baserar sig på användningen av tekniska system, i synnerhet sådana vilkas funktion är beroende av elenergi och datakommunikation. Enligt en bedömning i redogörelsen 2012 ökar också risken för störningar som påverkar samhället i stor utsträckning.

Redogörelsen 2012 betonar att Finland i alla förhållanden måste kunna garantera att samhällets vitala funktioner fortgår. Avvärjningen av de hot som överskrider gränserna och beredskapen inför sådana förutsätter enligt redogörelsen 2012 att såväl civila som militära resurser utnyttjas, att ett omfattande metodutbud används samt att Finland utvecklar sitt säkerhetstänkande i en mera övergripande riktning än tidigare. Ur säkerhetsmyndigheternas synvinkel är ett villkor för att man ska kunna svara på utmaningen att de gränsöverskridande hot som riktar sig mot den nationella säkerheten kan upptäckas och identifieras i ett tillräckligt tidigt skede.

2.2 Den nationella säkerhetspolitiska omgivningen

Det viktigaste intresset som samhället måste skydda kan anses vara statens självbestämmanderätt, med vilket avses statens suveränitet i förhållande till andra stater och rätt att på ett sätt som inte är beroende av andra använda sin högsta makt inom sina gränser. Andra centrala intressen som ska skyddas kan anses vara åtminstone ledningen av staten, internationell verksamhet, försvarsförmågan, den interna säkerheten, en fungerande ekonomi och infrastruktur samt befolkningens utkomstskydd och hand-

lingsförmåga.[1] De hot som riktar sig mot de intressen som nämns ovan kan anses äventyra den nationella säkerheten. De myndigheter som svarar för att hoten avvärjs kallas i detta betänkande nationella säkerhetsmyndigheter.

I och med internationaliseringen har gränsen mellan staternas yttre och inre säkerhet blivit allt diffusare. Det är också svårare än förr att avgränsa hoten och riskerna så att de binds till ett område eller en plats till följd av de ekonomiska, tekniska och sociala systemens statsgränsöverskridande art och ömsesidiga beroende. De allvarliga faktorer som hotar Finlands säkerhet anknyter numera ofta till händelser utanför Finland. Därmed kan ett hot av utländskt ursprung som uppkommit utomlands ha följder som lättare än tidigare realiseras också i Finland. De yttre hot som riktar sig mot den nationella säkerheten har det gemensamt att det är allt svårare att identifiera och urskilja de statliga eller icke-statliga parter som ligger bakom dem. Till följd av detta är det mera utmanande än tidigare att förutse hoten.

Grovt taget kan hoten delas in i civila och militära. Som centrala säkerhetshot av civil karaktär kan anses åtminstone internationell terrorism, spionage som främmande stater riktar mot Finland och landets intressen, strävanden att sprida massförstörelsevapen och produkter med dubbla användningsområden samt sådan internationell organiserad brottslighet som strävar efter att påverka det samhälleliga beslutsfattandet eller infiltrera statsstrukturerna. Under de senaste åren har i synnerhet sådant spionage som sker i datanätsomgivningen och är gränsöverskridande blivit ett betydande hot. En sådan verksamhet gör det möjligt att koncentrerat skaffa sig stora datamängder, vilket kan orsaka irreparabel skada för målstatens säkerhet och intressen.

Även de militära hoten har ändrat karaktär. Utöver traditionell militär verksamhet ingår i moderna militäroperationer olika slag av asymmetriska metoder. De moderna militäroperationerna börjar med påtrycknings- och desinformationsoperationer samt med datanätsattacker redan under fredstid. På detta sätt kan man medvetet sträva efter att påverka en annan stats beslutsfattande för att sådana strategiska slutmål ska kunna nås som den stat som är föremål för påtryckning annars inte skulle gå med på. I dagens värld utgör påtrycknings- och desinformationsoperationer en förlängning av staternas utrikes- och säkerhetspolitik. Också i militära operationer har icke-statliga aktörers påverkningsmöjligheter ökat i takt med den teknologiska utvecklingen och samhällets ökande sårbarhet.

Gränsen mellan politisk påverkan och krigföring blir diffusare när politiska och ekonomiska påtryckningsmetoder samt desinformationsoperationer används. I framtiden betyder inte heller en omfattande användning av våld nödvändigtvis att stora landområden tas i besittning. Målen kan man sträva efter att uppnå genom en överraskande våldsanvändning och en snabb erövring av begränsade områden.

[1] En säkerhetsstrategi för samhället s. 15

2.3 Den allt mera datatekniska kommunikationen

Informationen samt umgänget mellan människor har till stor del flyttat över till datanäten. Samhället har förvandlats till en miljö där nästan alla traditionella tjänster och funktioner styrs datatekniskt eller också har de helt och hållet flyttat ut på nätet. Datanäten fungerar enligt en annan logik än de gamla telefonnäten. Ett telefonsamtal reserverade det kretskopplade telefonnätet helt och hållet mellan den som ringde och den som svarade, i internet-nätet sker trafiken av otaliga kontakter omlott. Den sändande apparaten delar upp meddelandet i paket som den mottagande apparaten sammanställer till ett helt meddelande igen. Alla paket går inte nödvändigtvis enligt samma rutt till mottagaren, eftersom nätet sänder varje paket enligt den rutt som just då är mest kostnadseffektiv. Datakommunikationen mellan två parter i samma land kan ta rutten via en kontaktpunkt utomlands.

Utvecklingen i datanäten har möjliggjort t.ex. att molntjänster har blivit vanligare. I en molntjänst är det fråga om en depositionstjänst, där informationen är tillgänglig från vilken som helst apparat i nätet om man har innehavarrätten till informationen. De servrar som står i förbindelse med en molntjänst kan befinna sig inom en eller flera staters områden. Användaren har inte nödvändigtvis möjlighet att ta reda på var informationen deponerats fysiskt.

Med de säkerhetshot som riktar sig mot den nationella säkerheten sammanhänger, som en följd av globaliseringen, allt oftare kopplingar mellan personer i Finland och utomlands och det behov av ömsesidig kommunikation som följer av detta. De statliga och icke-statliga aktörer som står bakom hoten använder elektroniska medel i sin kommunikation, sitt uppdragsgivande, vid den rapportering som gäller realiserandet av uppdragen, vid planeringen av dåden, vid den informationsinhämtning som gäller målen, för att motivera och radikalisera deltagarna samt för att rekrytera nya medlemmar. En förutsättning för att hoten ska kunna avstyras på ett framgångsrikt sätt är att de myndigheter som ansvarar för den nationella säkerheten så tidigt som möjligt får kännedom om dessa kontakter och de omständigheter som behandlas inom ramen för dem och som äventyrar den nationella säkerheten. Tillgången till information på ett tidigt stadium förbättrar det finska samhällets förmåga att bemöta hoten och breddar därmed det metodutbud med hjälp av vilket man kan förhindra att hoten realiseras eller förbereda sig på dem. Den informationsinhämtning som de myndigheter som svarar för den nationella säkerheten har riktat in på kommunikationen i datanäten har globalt sett innehaft en central ställning vid förhindrandet t.ex. av terrordåd.

Nätverkandet i datanäten mellan de aktörer som hotar den nationella säkerheten kommer att öka i betydelse mera än tidigare. I takt med att de sociala medierna utvecklas blir sätten att nätverka mångsidigare. Terroristorganisationer och andra radikala organisationer satsar på att utveckla egna moderna medieorganisationer och på att sprida propaganda. De använder de sociala medierna allt mera vidsträckt, såsom direktkommunikationstjänster, samt upprätthåller öppna och stängda diskussionsforum. Dessa

möjliggör både lättanvänd kommunikation mellan två och flera personer och planering och samordning av aktionerna i realtid.

Enligt en bedömning i redogörelsen 2012 är statsaktörernas accentuerade militära förmågor bl.a. spanings- och övervakningssystem. Staterna utvecklar obemannade anordningar för spaning, övervakning och som lavetter för precisionsvapensystem. Den militära verksamhetsmiljön har förändrats. Främmande staters militära målsystem har blivit mera komplicerade, antalet signaler har ökat betydligt och en allt större del av datatrafiken går via datakommunikationskablar i stället för radiokanaler. Till följd av den förändrade verksamhetsmiljön har den finska militärunderrättelsens möjligheter att samla in underrättelseinformation blivit sämre.

Till följd av datateknikens snabba utveckling och lägre kostnader tar objekten för militärunderrättelsen i bruk flera kommunikationssystem än tidigare som är planerade för civil användning. Ledningen av väpnade styrkor stöder sig mera än tidigare på den allmänna datanätsstrukturen. I och med datateknikens framfart har mängden information som behandlas i datasystemen ökat betydligt och största delen av informationen finns numera i digital form. I dagens läge borde underrättelsen riktas mot den digitala informationen för att vara effektiv i den allt mera datatekniska omgivningen.

2.4 Datanätshot som riktas mot den nationella säkerheten

De parter som utgör ett hot mot den nationella säkerheten använder datanäten förutom för att kommunicera också som ett medel för att realisera hoten.

De hot som behandlas i strategin för cybersäkerheten i Finland och som äventyrar statens livsduglighet eller centrala säkerhetsintressen är framför allt cyberspionage, cyberterrorism och cyberoperationer. Det sist nämnda begreppet innehåller både påtryckning, en konflikt som realiseras i cyberomgivningen på en lägre nivå än ett krig och cyberoperationer som anknyter till krig.

Genom cyberspionage skaffas information som är klassificerad på samma sätt som en stats- eller företagshemlighet eller sensitiv information ur datasystemen.[2] Spionage i cyberomgivningen kan fortgå till och med i åratal utan att det upptäcks. Enligt bedömning från säkerhetsmyndigheterna försöker flera främmande stater rikta omfattande och tekniskt avancerat cyberspionage mot den finska statsförvaltningen och de företag som är av samhällsekonomisk betydelse. I cyberspionage används inte ett vanligt skadeprogram, som kan upptäckas med ett kommersiellt virusbekämpningsprogram, utan ett tekniskt utvecklat och mångsidigt verktyg för nätattacker. Verktygets

[2] Som exempel på informationsinhämtning och påverkan som sker via cyberomgivningen kan nämnas skadeprogrammet Stuxnet som riktades mot Irans kärnprogram samt laddningsfilerna Red October och Agent.btz, vilka hittats i nät hos försvarsförvaltningarna i Ukraina, flera europeiska stater och Förenta staterna samt spionageprogrammen Snake, Turla och Uroboros som vidareutvecklats framför allt ur Agent.btz.

första uppgift är att ta i besittning en viss del av nätet och nästa uppgift att installera mera utvecklade attackberedda spionage- och skadeprogram. En spionageoperation är på förhand noggrant planerad och den har ett exakt operativt mål som är att samla information t.ex. om omständigheter som är förknippade med målstatens utrikes- och säkerhetspolitik, ekonomi och industri. Utöver underrättelseprogrammen kan i datasystem också infiltreras skadeprogram som aktiveras när en kris börjar. Nya teknologier skapar nya möjligheter till krigföring med hjälp av cyberoperationer, vilkas verkningar drabbar hela samhället, inte enbart stridskrafterna.

Cyberspionage och cyberoperationer kommer att få ännu större betydelse under de kommande åren. Skälen till detta är möjligheten att genomföra dåd i cyberomgivningen till låga kostnader, svårigheten och de höga kostnaderna för att skydda sig samt de små riskerna att åka fast. Alla de främmande makter som är väsentliga med tanke på hur Finlands säkerhetspolitiska omgivning utvecklas satsar också målmedvetet och ansenligt på att bygga upp sin offensiva cyberkapacitet. Som exempel på cyberoperationer som riktats mot stater kan nämnas nätattacker mot slutna myndighetsnät i Ukraina (2014), Georgien (2008) och Estland (2007). Dessa operationer visade sig vara väl organiserade och planerade, och det bedöms att bakom dem står en statsaktör eller parter som är mycket nära kopplade till en stat.

Hotet om cyberattacker som genomförs i terroristiskt syfte mot Finland är fortfarande begränsat. Situationen kan emellertid ändras snabbt som en följd av utvecklingen i den internationella omgivningen. Vissa internationella terroristgrupper har strävat efter att utveckla sin cyberattackförmåga och i fråga om flera grupper finns det antydningar om strävanden både att utveckla det egna kunnandet och att utlokalisera det (precisionsattacker som realiseras i form av köpta tjänster). Som möjliga gärningar kommer i fråga överbelastningsattacker, vilka skadar tillgången på kritiska nättjänster, samt det förstörelsearbete som gjorts via kontrollrumssystemet SCADA och som i värsta fall orsakar ansenliga skador på person och egendom.

2.5 Om datanätskriminalitet

De hot som datanätskriminaliteten medför har varit starkt på uppåtgående under de senaste åren. Brotten kan riktas mot enskilda medborgare, företag och andra sammanslutningar eller mot hela samhället. Detta kan ses i fråga om de datanätsbrott som kommit till polisens kännedom både som ett ökande antal och i det att gärningarna har blivit allt skadligare. Enligt UNODC, som är ett FN-organ, blir medborgarna mera sannolikt offer vid datanätsbrott än vid traditionella brott.

Datanätskriminaliteten är till en stor del en dold brottslighet, som inte kommer till polisens kännedom och ofta upptäcker inte heller de berörda det som har inträffat. Om de gör det, kan det gå en lång tid till dess och ofta behandlar de saken utan att anmäla den till myndigheterna eller ens till eventuella kunder.

Datanätskriminaliteten är internationell. Brottsförövarna agerar ofta i olika grupper, som bildas av dem som har den kunskap och de resurser som behövs. Förövarna på internet känner inte varandras verkliga identitet. De agerar var och en i sitt land och använder resurser och tjänster från olika länder för att begå brotten och inriktar attackerna på flera länder samtidigt. Mål kan vara system som är kritiska för samhället, såsom t.ex. internationella bank- och betalningsrörelsesystem.

När man har misstänkt ett allvarligt brott har det inte alltid nödvändigtvis varit fråga om ett avsiktligt brott utan det kan ha varit ett programfel, apparatfel, en fel konfigurerad apparat eller ett annat mänskligt fel eller också har man kanske inte genast kunnat konstatera vem som står bakom brottet eller vilket motivet är.

3 NULÄGET I FRÅGA OM INFORMATIONSINHÄMTNINGEN OCH AVVÄRJNINGEN AV HOT MOT DATASÄKERHETEN

3.1 De lagstadgade uppgifterna för de myndigheter som svarar för den nationella säkerheten

3.1.1 Om polisens uppgifter och befogenheter

Det är polisens uppgift att trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning. Polisen ska upprätthålla säkerheten i samarbete med övriga myndigheter samt med sammanslutningar och invånare och sköta det internationella samarbete som hör till dess uppgifter.

Bestämmelser om polisens befogenheter att inhämta den information som behövs för att förhindra och avslöja brott finns i polislagen. Bestämmelser om polisens befogenheter att inhämta den information som behövs för att reda ut brott ingår igen i tvångsmedels- och förundersökningslagarna. I de totalreviderade polis- och tvångsmedelslagarna, som trädde i kraft år 2014, harmoniserades lagarnas reglering av olika slag av informationsinhämtningsbefogenheter, vilket gör att båda lagarna innehåller bestämmelser som gäller i stora drag samma metoder för informationsinhämtning. En central skillnad är det syfte i vilket metoderna att inhämta information används: å ena sidan i syfte att förhindra och avslöja brott (polislagen) och å andra sidan i syfte att reda ut brott (tvångsmedelslagen).

I 4 kapitlet i polislagen föreskrivs om polisens rätt att få information. Enligt 2 § 1 mom. i kapitlet har polisen rätt att för tjänsteuppdrag få behövlig information och handlingar av myndigheter och sammanslutningar som tillsatts för att sköta offentliga uppgifter, oberoende av tystnadsplikten, om inte överlämnande av informationen eller handlingarna till polisen eller användning av informationen som bevis uttryckligen har förbjudits eller

begränsats i lag. Enligt 3 § 1 mom. i samma kapitel har polisen rätt att få information som behövs för förhindrande eller utredning av brott oberoende av företags-, bank- eller försäkringshemlighet. Enligt 2 mom. har en polisman i enskilda fall rätt att av teleföretag och av sammanslutningsabonnenter få kontaktuppgifter för teleadresser som inte är upptagna i en offentlig katalog eller information som specificerar en teleadress eller teleterminalutrustning, om informationen behövs för ett polisuppdrag.

3.1.1.1 Skyddspolisens uppgifter

I polisens organisation svarar Skyddspolisen, som är en riksomfattande enhet, för avvärjningen av hot som riktas mot den nationella säkerheten. Enligt 10 § i polisförvaltningslagen har Skyddspolisen till uppgift att bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet samt att utföra undersökning av sådana brott. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att förebygga verksamhet som äventyrar rikets säkerhet. Polisstyrelsen bestämmer närmare om de ärendegrupper som Skyddspolisen ska undersöka. Enligt regeringens proposition gällande polisförvaltningslagen (RP 155/1991 rd) har man i sättet att utforma bestämmelserna strävat efter att beakta den accentuerade betydelsen av den förebyggande verksamheten på Skyddspolisens uppgiftsområde. Enligt förarbetet intar förebyggandet av dåd som äventyrar rikets säkerhet en särskilt central plats i Skyddspolisens arbete, medan igen inriktandet av undersökning på ett intrång i säkerhetsintressen som redan har skett i allmänhet är ett bevis på att den förebyggande verksamheten till någon grad har misslyckats.

Sätten att realisera den förebyggande uppgift som har föreskrivits för Skyddspolisen preciseras i polisförvaltningsförordningen (158/1996). Enligt 8 § i förordningen ska Skyddspolisen, för att fullgöra den uppgift som bestäms i polisförvaltningslagen, i enlighet med de allmänna grunder som fastställts av ministeriet meddela myndigheter och samfund sådana anvisningar, råd och upplysningar som behövs för upprätthållande av statens säkerhet eller för att förhindra att den kränks.

Polisförvaltningslagens 10 § fastställer Skyddspolisens verksamhetsområde genom att räkna upp de rättsgoda – rikets inre och yttre säkerhet, stats- och samhällsskicket – som Skyddspolisen har till uppgift att skydda. Sådana konkreta fenomen och säkerhetshot som det ankommer på Skyddspolisen att bekämpa nämns inte i lagen. Genom att definiera uppgifterna med utgångspunkt i rättsgoda har man uppenbarligen velat garantera att Skyddspolisens verksamhet för att skydda statens centrala säkerhetsintressen kan anpassas till förändrade förhållanden samt att ämbetsverkets verksamhetsområde gällande bekämpningen är generellt.

Skyddspolisens verksamhetsområde konkretiseras i Polisstyrelsens föreskrift om Skyddspolisens uppgifter och samverkan med den övriga polisen. Denna föreskrift förnyas med bestämda intervaller. Enligt den nuvarande föreskriften är Skyddspolisens huvuduppgifter:

- att avvärja, förebygga och avslöja terrorism
- att avvärja, förebygga och avslöja olaglig underrättelseverksamhet
- säkerhetsarbete

Vidare är Skyddspolisens uppgift enligt föreskriften bl.a.:

- att förhindra spridningen av massförstörelsevapen i samarbete med andra myndigheter
- att analysera statens säkerhetspolitiska omgivning
- att upprätthålla en nationell och internationell lägesbild inom sitt verksamhetsområde
- att avvärja, förebygga och avslöja olaglig aktivism i anslutning till statens inre säkerhet
- att bedöma hot i anslutning till statsbesök och andra storskaliga möten
- att utföra den säkerhetsunderrättelse som hör till verksamhetsområdet
- att undersöka vissa brott som hör till verksamhetsområdet

Skötseln av de uppgifter som har föreskrivits för Skyddspolisen inbegriper aktiv bevakning av den finska säkerhetspolitiska omgivningen, att inhämta förutseende information gällande säkerhetshot och att analysera den information som inhämtats. Informationen analyseras i första hand för den högsta statsledningens behov. I 4 a § i polisförvaltningslagen sägs att Skyddspolisen ska underrätta inrikesministern och polisöverdirektören om sådana angelägenheter i Skyddspolisens uppgifter som är av samhällelig betydelse. Enligt motiveringarna till denna bestämmelse är Skyddspolisen skyldig att underrätta också republikens president, statsministern och utrikesministern med beaktande av de utrikes- och säkerhetspolitiska uppgifter som föreskrivs för dem. Dessutom ska Skyddspolisen också informera riksdagens grundlags-, förvaltnings- och utrikesutskott om hur säkerhetsläget i Finland utvecklas.

I takt med att säkerhetshoten blir mera komplicerade och internationella behövs allt mera underrättelsematerial med allt högre kvalitet som stöd för det politiska beslutsfattandet. Antalet rapporter från Skyddspolisen som har utarbetats för den högsta statsledningen och beskriver Finlands säkerhetsläge har tiofaldigats sedan år 2008.

Vid inrikesministeriet pågår just nu en ändring av Skyddspolisens administrativa ställning så att Skyddspolisen i stället för att som nu vara underställd Polisstyrelsen ska vara en polisenhet direkt underställd inrikesministeriet. Enligt utkastet till regeringsproposition om detta kommer ändringen bl.a. att stärka den politiska partens strategiska styrning av Skyddspolisens verksamhet och förtydliga Skyddspolisens ställning både inom det inhemska myndighetsfältet och i det internationella samarbetet mellan säkerhets- och underrättelsetjänsterna, vilket blir allt viktigare. Genom ändringen minskar Skyddspolisens administrativa avstånd till de säkerhetspolitiska beslutsfattarna och förtydligas Skyddspolisens direkta samarbets- och rapporteringsrelationer. Målet är att utöka statsledningens möjligheter att påverka hur Skyddspolisens informat-

ionsinhämtning inriktas och därmed förbättra Skyddspolisens förmåga att producera information som betjänar Finlands inre säkerhet och utrikes- och säkerhetspolitiska beslutsfattande.

Det mål som gäller förbättrandet av betjäningsförmågan sammanhänger nära med frågan om att forma en bestående styrnings- och samordningsmekanism på ministerienivå för att inrikta Skyddspolisens informationsinhämtning. En arbetsgrupp som har rett ut Skyddspolisens administrativa ställning och resultatstyrning samt utvecklandet av övervakningen kom i sin slutrapport, som överräcktes till inrikesministern den 24 september 2014 (inrikesministeriets publikationer 28/2014), med ett förslag om att en sådan mekanism ska bildas. Enligt förslaget ska för Skyddspolisens verksamhet årligen ställas prioriteringar i fråga om informationsinhämtningen under ledning av det ministerium som styr ämbetsverkets verksamhet. Innan prioriteringarna slås fast ska de behandlas i förberedande och samordnande grad till exempel i statsrådets utrikes- och säkerhetspolitiska ministerutskott samt en utredning om dem ska ges till utskotten i fråga i riksdagen. Det har bedömts att genomförandet av mekanismen inte förutsätter författningsändringar på lagnivå.

3.1.2 Försvarsmaktens uppgifter

Enligt 2 § i lagen om försvarsmakten hör det militära försvaret av Finland, stödjande av andra myndigheter samt deltagande i militär krishantering till försvarsmaktens uppgifter. Enligt 2 § 1 mom. 1 a punkten i lagen om försvarsmakten innefattar det militära försvaret av Finland övervakning av landområdena, vattenområdena och luftrummet samt tryggande av den territoriella integriteten. Enligt 2 § 1 mom. 1 b punkten i lagen om försvarsmakten innefattar det militära försvaret av Finland också tryggande av befolkningens livsbetingelser, de grundläggande fri- och rättigheterna och statsledningens handlingsfrihet samt försvar av den lagliga samhällsordningen.

I statens suveränitet ingår dess territoriella integritet. I territorialövervakningslagen (755/2000) ingår bestämmelser om övervakning och tryggande av Finlands territoriella integritet. Genom territorialövervakningen förebyggs eller uppdagas och klarläggs territorieförseelser och territoriekränkningar. Med stöd av lagen har närmare bestämmelser getts i statsrådets förordning om territorialövervakning (971/2000).

I territorialövervakningslagen definieras en främmande stats fientliga verksamhet i 34 § 4 och 5 punkten bl.a. enligt följande:

> ”4) spaning och elektronisk störning som av en främmande stat orättmätigt riktas mot på finskt territorium belägna objekt som är viktiga med tanke på rikets säkerhet,

5) elektronisk störning som av en främmande stat orättmätigt riktas mot ett finländskt statsluftfartyg eller statsfartyg som utför ett territorialövervakningsuppdrag.”

Försvarssystemet har till uppgift att forma och upprätthålla den militärstrategiska lägesbild som beslutsfattandet förutsätter. Militärunderrättelse som en del av försvarsmaktens uppgifter nämns i detaljmotiveringen till 2 § i lagen om försvarsmakten (RP 264/2006 rd, s. 17–18). I motiveringarna till 2 § 1 mom. 1 b punkten i lagen konstateras att ”försvarsmakten tryggar för sin del folkets livsbetingelser och de grundläggande fri- och rättigheterna, statsledningens handlingsfrihet och den lagliga samhällsordningen. - - För att tryggandet av dessa skall vara möjligt måste försvarsförmågan vara tillräcklig. Dessutom skall försvarsmakten förebygga militära hot och avvärja anfall mot landet.” Dessutom har det konstaterats i motiveringstexten till 2 § i lagen att ”för att skapa och upprätthålla en militärstrategisk lägesbild måste underrättelse- och övervakningssystemet följa upp utvecklingen inom Finlands säkerhetsmiljö, fastställa förändringar i miljön och producera information om den rådande situationen. Systemet ger en förvarning om utvecklingen av militära hot, så att behövliga motåtgärder kan inledas.” Målet för militärrunderrättelse är huvudsakligen statsaktörer, i synnerhet utländska militärorganisationer.

Det finns emellertid ingenting föreskrivet om militärunderrättelsens befogenheter. Däremot finns det bestämmelser om försvarsmaktens kontraunderrättelseuppdrag, dvs. förebyggande och avslöjande på finskt område av brott med anknytning till verksamhet som äventyrar syftet med försvaret i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014).

3.2 Skyddspolisens och försvarsmaktens informationsinhämtning inom landet

3.2.1 Skyddspolisens informationsinhämtning inom landet

3.2.1.1 Allmänt

Skyddspolisens viktigaste uppgift är att förebygga och avslöja förehavanden och brott som är kopplade till terrorism, olaglig underrättelseverksamhet, spridning av massförstörelsevapen och extremrörelser samt till organiserad brottslighet som äventyrar statens säkerhet samt i begränsad utsträckning också att undersöka brott som anknyter till ovan nämnda fenomen. För att uppgiften ska kunna utföras förutsätts att Skyddspolisen kan inhämta information om sådana förehavanden och brott.

För att inhämta sådan information som är offentligt tillgänglig krävs i allmänhet inte någon särskilt stadgad myndighetsbefogenhet som grund. Eftersom de förehavanden och brott som Skyddspolisen ska avvärja förbereds i hemlighet, kan man i praktiken inte grunda bekämpningsåtgärderna på den information som finns att tillgå offentligt. En central roll intar därmed den verksamhet som siktar till att inhämta annan inform-

ation än den som är allmänt tillgänglig. För att vara effektiv ska informationsinhämtningen dessutom utföras i hemlighet för sitt objekt.

För Skyddspolisen har inte föreskrivits några särskilda befogenheter för inhämtning av information om hot med anknytning till statens säkerhet. Skyddspolisen är en polismyndighet som i sin verksamhet använder sig av de befogenheter att inhämta information och andra befogenheter som har föreskrivits för polisen.

I Skyddspolisens praktiska verksamhet är de i polislagen föreskrivna hemliga metoderna för inhämtande av information för att förhindra och avslöja ett brott viktiga. De uppgifter som gäller utredning av brott begränsas för Skyddspolisens del i praktiken främst till undersökning av brott med anknytning till olaglig underrättelseverksamhet. Skyddspolisen utför endast sällan förundersökning.

3.2.1.2 Begreppen för förebyggande och avslöjande av brott

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

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

Enligt 5 kap. 1 § 3 mom. i polislagen avses med *avslöjande av brott* åtgärder som syftar till att klarlägga om det för inledande av förundersökning finns en i 3 kap. 3 § 1 mom. i förundersökningslagen avsedd grund[3], när det utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet kan antas

[3] Enligt 3 kap. 3 § 1 mom. i förundersökningslagen ska förundersökningsmyndigheten göra förundersökning när det på grund av anmälan till den eller annars finns skäl att misstänka att ett brott har begåtts.

att ett brott har begåtts. Begreppet avslöjande av brott avser gråzonen mellan förhindrande respektive utredning av brott. Det är inte fråga om brottsutredning eftersom förutsättningar för inledande av förundersökning saknas, men inte heller förhindrande av brott, eftersom brottet redan antas ha blivit begånget. Som exempel kan nämnas den situationen att man fått tips om att ett brott redan har begåtts men det inte finns någon konkret grund för misstanken och inte heller någon sådan orsak att misstänka brott som avses i förundersökningslagen. (RP 224/2010 rd, s. 93).

3.2.1.3 Förutsättningarna för att hemliga metoder för inhämtande av information ska få användas

I 5 kapitlet i polislagen ingår bestämmelser om de metoder för inhämtande av information som polisen – inklusive Skyddspolisen – får använda för att i hemlighet inhämta information om en person som är föremål för åtgärden.
Dessa metoder är

- teleavlyssning (polislagen 5 kap. 5 §)
- inhämtande av information i stället för teleavlyssning (polislagen 5:6)
- teleövervakning (polislagen 5:8)
- teleövervakning med samtycke av den som innehar teleadress eller teleterminalutrustning (polislagen 5:9)
- inhämtande av basstationsuppgifter (polislagen 5:11)
- systematisk observation (polislagen 5:13)
- förtäckt inhämtande av information (polislagen 5:15)
- teknisk avlyssning (polislagen 5:17)
- optisk observation (polislagen 5:19)
- teknisk spårning (polislagen 5:21)
- teknisk observation av utrustning (polislagen 5:23)
- inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning (polislagen 5:25)
- täckoperationer (polislagen 5:28)
- bevisprovokation genom köp (polislagen 5:35)
- användning av informationskällor och styrd användning av informationskällor (polislagen 5:40)
- kontrollerade leveranser (polislagen 5:43)

De hemliga metoderna för inhämtande av information kan grupperas på olika sätt enligt användningssätt och syfte. En del av dem är tekniska metoder för inhämtande av information, vilka riktas på målpersonens kommunikation, medan igen andra kan beskrivas som metoder för inhämtande av information om en person. Vidare kan metoderna för inhämtande av information grupperas t.ex. enligt huruvida metoden för inhämtande av information förutsätter direkt växelverkan mellan användaren och målpersonen och att målpersonen förs bakom ljuset eller inte. Förtäckt inhämtande av information, täckoperationer och bevisprovokation genom köp baserar sig på en sådan vilseledande direkt växelverkan, medan igen information om målpersonen i informat-

ionskällor och styrd användning av informationskälla inhämtas via mellanhänder. Systematisk observation baserar sig på iakttagelser av målpersonens beteende utgående från sinnesintryck.

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

För användningen av olika metoder för inhämtande av information har i polislagen ställts s.k. allmänna förutsättningar och särskilda förutsättningar. Särskilda förutsättningar för användningen av hemliga metoder för inhämtande av information är framför allt de specificerade brott, för vilkas förhindrande varje metod kan användas. I bestämmelserna om de olika metoderna för inhämtande av information har det också kunnat ställas andra särskilda förutsättningar. I sammandrag kan det konstateras att Skyddspolisen så gott som helt kan använda de hemliga metoder för inhämtande av information om vilka föreskrivs i 5 kapitlet i polislagen för att förhindra terrorismbrott vilka enligt 34 a kapitlet i strafflagen är straffbara och för att förhindra brott med anknytning till olaglig underrättelseverksamhet vilka enligt 12 kapitlet i strafflagen är straffbara. I fråga om förhindrandet av brott som syftar till att sprida massförstörelsevapen och produkter med dubbla användningsområden liksom också brott som anknyter till organiserade kriminella gruppers verksamhet och äventyrar statens säkerhet är situationen mera mångdimensionell och kontroversiell.

De hemliga metoder för inhämtande av information som nämns ovan kan användas för avslöjande av brott endast om det är fråga om ett landsförräderi- eller terroristbrott om vilket föreskrivs närmare i lag. I samband med avslöjandet av brott tillämpas inte de särskilda förutsättningar om vilka föreskrivs i de metodvisa bestämmelserna gällande hemliga metoder för inhämtande av information (RP 224/2010 rd, s.92)

Valet och användningen av de hemliga metoderna för inhämtande av information styrs av de allmänna principer om vilka föreskrivs i 1 kapitlet i polislagen, såsom principen om respekt för de grundläggande rättigheterna och de mänskliga rättigheterna, proportionalitetsprincipen, principen om minsta olägenhet och principen om ändamålsbundenhet.

Ett gemensamt drag för de hemliga metoderna för inhämtande av information är att de har definierats utgående från person och brott. De kan endast riktas mot en sådan person eller användas för inhämtande av information om en sådan persons verksamhet, som av grundad anledning kan antas i framtiden göra sig skyldig eller redan ha gjort sig skyldig till ett brott av en viss allvarlighetsgrad eller till förberedande av ett sådant. Om det inte föreligger en sådan brottsavvärjande grund i anknytning till en viss person, är det inte möjligt att använda en hemlig metod för inhämtande av information i enlighet med polislagen. Inhämtande av annan underrättelseinformation måste således grunda sig på bevakningen av öppna källor, polisens s.k. allmänna övervakning samt på information som Skyddspolisen får via sitt samarbetsnätverk av andra myndigheter och av privata sammanslutningar.

3.2.1.4 Avvärjning av förehavanden

Enligt 10 § i polisförvaltningslagen bekämpar Skyddspolisen utöver brott som äventyrar rikets säkerhet också förehavanden som äventyrar den. Begreppet förehavande preciseras varken i polisförvaltningslagen eller i förarbetet till den. Av det att Skyddspolisens hemliga metoder för inhämtande av information grundar sig på brott följer att de inte kan användas för att inhämta information om sådana förehavanden som äventyrar rikets säkerhet men som ännu inte har framskridit till åtminstone stadiet förberedelse av brott.

Den arbetsgrupp som redde ut Skyddspolisens administrativa ställning och resultatstyrning samt utvecklande av övervakningen behandlade i sin slutrapport, som avläts till inrikesministern den 24 september 2014, frågan om ifall Skyddspolisens befogenheter att inhämta information kunde utsträckas till att gälla också avvärjande av förehavanden. Enligt arbetsgruppens slutrapport måste nya underrättelsebefogenheter övervägas för Skyddspolisen för att den ska kunna svara mot sin förändrade verksamhetsmiljö. Det vore fråga om att av personer som agerar informationskällor och från datanät inhämta information som är nödvändig för avvärjande av förehavanden som äventyrar rikets säkerhet, även om förehavandena inte har framskridit till det stadiet att de utgör brott som ska förhindras, avslöjas eller utredas. Enligt arbetsgruppen måste man, när man överväger saken, närmare reda ut de juridiska förutsättningarna för en möjlig utvidgning av underrättelsebefogenheterna bland annat med tanke på de grundläggande rättigheterna och de mänskliga rättigheterna.

3.2.2 Försvarsmaktens inhämtning av information inom landet

Militärunderrättelsen riktar in sig på Finlands yttre verksamhetsmiljö. Ur funktionell synvinkel bör militärunderrättelse avskiljas från militär kontraunderrättelse som försvarsmakten utför som ett polisuppdrag av brottsbekämpningsskäl. Vid militär kontraunderrättelse är det fråga om att förebygga och avslöja brott på finskt territorium. Med militär kontraunderrättelse avses förebyggande och avslöjande av brott med anknytning till verksamhet som äventyrar syftet med det militära försvaret och olovlig underrättelseverksamhet, vilka riktas mot Finland inom området för militärt försvar.

Genom militär kontraunderrättelse förhindras främmande staters inhämtning av information i Finland t.ex. om försvarsmaktens kapaciteter och sammansättningar, vilken riktas mot Finland och är kriminaliserad i finsk strafflag. Typiska brottsbenämningar som är föremål för förebyggande och avslöjande är de landsförräderibrott som avses i 12 kapitlet i strafflagen, såsom landsförräderi, spionerі och olovlig underrättelseverksamhet, och högförräderibrott som avses i 13 kapitlet. Också vanligare brott, såsom egendomsbrott, kan emellertid vara föremål för förebyggande och avslöjande, ifall de sammanhänger med underrättelseverksamhet som riktas mot Finland inom det militära försvarets område och verksamhet som äventyrar syftet med det militära försvaret. Exempel på dylika är ett datasäkerhetsbrott eller egendomsbrott som riktas mot försvarsmaktens sekretessbelagda information. Någon uttömmande förteckning över de brott som befogenheten ska gälla har det inte föreskrivits om.

Inom försvarsförvaltningens område bestäms om försvarsmaktens uppgift gällande militär kontraunderrättelse i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Försvarsmakten är en specialmyndighet i fråga om kontraunderrättelse, som har till uppgift att inom det militära försvarets område sörja för förebyggandet och avslöjandet av brott med anknytning till underrättelseverksamhet riktad mot Finland och verksamhet som äventyrar syftet med det militära försvaret utan att detta begränsar den behörighet som i lag har föreskrivis för Skyddspolisen. Försvarsmaktens behörighet i fråga om att förebygga och avslöja brott är mera begränsad än den allmänna behörighet som har föreskrivits för Skyddspolisen i 10 § i polisförvaltningslagen. Försvarsmaktens behörighet gäller endast de brott som sammanhänger med underrättelseverksamhet riktad mot Finland och verksamhet som äventyrar syftet med det militära försvaret inom området för det militära försvaret. Inom detta område är behörigheten parallell med Skyddspolisens allmänna behörighet i fråga om förebyggandet och avslöjandet av brott, men den begränsar inte Skyddspolisens allmänna behörighet. I lagen har inbegripits rätt för polisen att på eget initiativ från försvarsmakten ta över skötseln av ett ärende gällande förebyggande och avslöjande av ett brott.

Vid förebyggandet och avslöjandet av brott följs också vid försvarsmakten de principer om vilka föreskrivs i polislagen och av dem i synnerhet principen om respekt för de grundläggande rättigheterna och de mänskliga rättigheterna, proportionalitetsprincipen, principen om minsta olägenhet och principen om ändamålsbundenhet. Skyddspolisen svarar för utredningen av ett brott som kommit fram vid försvarsmaktens militära kontraunderrättelse.

I fråga om befogenheterna för de tjänstemän vid försvarsmakten som sköter förebyggandet och avslöjandet av brott gäller enligt lagen om militärdisciplin och brottsbekämpning inom försvarsmakten vad som i polislagen föreskrivs om befogenheter att förebygga och avslöja brott. I fråga om de hemliga metoderna för inhämtande av information har försvarsmakten dock endast följande begränsade del av polisens befo-

genheter till sitt förfogande: 1) inhämtande av basstationsuppgifter, 2) systematisk observation, 3) förtäckt inhämtande av information, 4) teknisk avlyssning, 5) optisk observation, 6) teknisk spårning, 7) inhämtande av identifieringsuppgifter för teleadresser och teleterminalutrustning. Dessutom får i enlighet med den tilläggsavgränsning som gäller uppgiften att avslöja brott dessa åtgärder för inhämtande av information användas vid avslöjandet av brott endast när det är fråga om äventyrande av Finlands suveränitet, krigsanstiftan, landsförräderi eller grovt landsförräderi, spionerі eller grovt spionerі, röjande av statshemlighet eller avslöjande av ett brott som gäller olovlig underrättelseverksamhet. En tjänsteman vid försvarsmakten som sköter förebyggande och avslöjande av brott ska meddela Skyddspolisen att ovan nämnda hemliga metoder för inhämtande av information används.

I lagen om militär disciplin och brottsbekämpning inom försvarsmakten föreskrivs om den assistans som polisen ger när de som sköter brottsbekämpningen inom försvarsmaken inte har befogenhet att utföra en åtgärd som är nödvändig för skötseln av uppgifterna. I praktiken är det fråga om att inhämta information med en sådan befogenhet som polisen har till sitt förfogande och som försvarsmakten inte har rätt att använda. Förebyggandet och avslöjandet av brott genomförs av tjänstemän som är placerade vid huvudstaben och vid Försvarsmaktens underrättelsetjänst som är underställd den.

3.3 Skyddspolisens och försvarsmaktens inhämtande av information gällande utlandet

3.3.1 Skyddspolisens inhämtande av information gällande utlandet

Enligt 10 § i polisförvaltningslagen har Skyddspolisen till uppgift att bekämpa bl.a. hot som kan äventyra rikets yttre säkerhet. Hot av utländskt ursprung som därmed hotar statens yttre säkerhet är bl.a. internationell terrorism, främmande staters spionerі som de riktar mot Finland och landets intressen samt spridning av massförstörelsevapen. Enligt Skyddspolisens uppgiftsförordnande är det ämbetsverkets uppgift också att analysera statens säkerhetspolitiska omgivning och att upprätthålla en internationell lägesbild inom sitt verksamhetsområde. Skyddspolisen rapporterar till Finlands högsta statsledning hur den internationella säkerhetspolitiska omgivningen utvecklar sig.

Betänkandet av den parlamentariska poliskommittén (kommittébetänkande 1986:16) som låg till grund för stiftandet av polisförvaltningslagen, betonar att av statens självständighet följer att den måste ha beredskap att hela tiden skydda sin yttre säkerhet. Enligt betänkandet kan den yttre säkerheten äventyras av alla sådana strävanden som har en skadlig inverkan på rikets rättigheter och intressen eller på relationerna mellan Finland och främmande stater. Enligt den parlamentariska poliskommittén är det uttryckligen Skyddspolisen som har en central roll vid avvärjandet av dylika faror och olägenheter. Finlands säkerhetspolitiska omgivning har internationaliserats kraftigt efter offentliggörandet av den parlamentariska poliskommitténs betänkande. Information om andra län-

der har en allt större betydelse vid skyddandet av de säkerhetsintressen som Skyddspolisen ansvarar för.

Det finns ingenting föreskrivet i lag om Skyddspolisens inhämtande av information utomlands. Skyddspolisens inhämtande av information grundar sig på användning av de befogenheter som gäller förhindrande och avslöjande av brott i enlighet med polislagen. Dessa befogenheter kan Skyddspolisen använda endast på finskt territorium. Skyddspolisens möjligheter att få information om utlandet stöder sig i praktiken på det internationella underrättelsesamarbete som Skyddspolisen idkar, på bevakningen av öppna källor samt på Skyddspolisens verksamhet med egna kontaktpersoner.

Skyddspolisen och dess föregångare har sedan Finland blev självständigt bedrivit ett omfattande bilateralt och multilateralt samarbete med utländska underrättelse- och säkerhetstjänster. Med hjälp av samarbetet säkerställs att den utländska underrättelseinformation som är nödvändig för att statens säkerhet ska kunna upprätthållas kan ställas till de finska behöriga myndigheternas förfogande. Till följd av säkerhetsfrågornas allmänna globaliseringsutveckling och den ökande betydelsen av utländsk underrättelseinformation som blev följden av detta har Skyddspolisen under de senaste åren planenligt breddat sitt internationella samarbetsnätverk så att det för närvarande anses täcka underrättelse- och säkerhetsorganen i alla länder som är viktiga med tanke på Finlands säkerhet.

De internationella samarbetsförfaranden som betjänar brottsbekämpningen måste hållas isär från det internationella underrättelsesamarbetet. Inom Skyddspolisens verksamhetsområde är betydelsen av dessa samarbetsförfaranden liten. Ett centralt skäl till detta är att målpersonerna för den brottsbekämpning som Skyddspolisen idkar i allmänhet agerar för en främmande stats räkning, ofta även som tjänstemän i denna stat, mot Finlands intressen. En stat som drar nytta av en brottslig gärning ger i praktiken inte sådan hjälp som behövs för att förhindra, avslöja eller reda ut brottet till den stat - t.ex. Finland - som brottet riktar sig mot.

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

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

Den arbetsgrupp som redde ut Skyddspolisens administrativa ställning och resultatstyrning samt utvecklandet av övervakningen föreslog i sin slutrapport att det skulle övervägas om Skyddspolisens underrättelsebefogenheter borde utvecklas. Av arbetsgruppens slutrapport framgår att den förändring av verksamhetsmiljön som ligger till grund för behoven av befogenheter gäller framför allt Finlands yttre säkerhetspolitiska omgivning. Arbetsgruppens förslag, enligt vilket Skyddspolisen borde kunna inhämta information för att bekämpa förehavanden som äventyrar rikets säkerhet med hjälp av verksamhet som gäller informationskällor, gäller också verksamhet utomlands.

3.3.2 Försvarsmaktens inhämtande av information gällande utlandet

Militärunderrättelse som en del av försvaret

Den militära underrättelseverksamhet som ska bedrivas av försvarsmakten i dess försvarsuppgift har traditionellt ansetts basera sig på försvarsmaktens lagstadgade uppgift att försvara rikets självständighet och territoriella integritet. Då har militärunderrättelse ansetts vara inbegripen i 2 § 1 mom. 1 a och 1 b punkten i lagen om försvarsmakten och den har inte nämnts särskilt i lagen.

Militärunderrättelse riktar sig mot Finlands yttre verksamhetsmiljö. Militärunderrättelsens uppgift är att forma och upprätthålla den militärstrategiska lägesbild som det militära beslutsfattandet förutsätter. För att forma denna bild följer militärunderrättelsen med utvecklingen i Finlands säkerhetspolitiska omgivning, fastställer förändringarna i omgivningen och sammanställer information om det rådande läget. Genom militärunderrättelsen upprätthåller och utvecklar försvarsmakten försvarsberedskapen. Mål för militärunderrättelsen är huvudsakligen statsaktörer. Syftet med militärunderrättelsen är att forma och upprätthålla medvetenheten om verksamhetsmiljön. Det centrala är förmågan att ge en förvarning om att militära hot håller på att utveckla sig så att den högsta statsledningens beslutsfattande om Finlands säkerhet i fråga om hot som äventyrar Finlands suveränitet grundar sig på lägesinformation i rätt tid och vid behov gör det möjligt att vidta beredskaps- och motåtgärder i rätt tid.

Det finns inga bestämmelser i lag om militärunderrättelsens befogenheter att inhämta information. Militärunderrättelsen har organiserats inom försvarsmakten genom interna föreskrifter och anvisningar.

Försvarsmakten bedriver det samarbete som verksamheten förutsätter med utländska underrättelsemyndigheter. Genom samarbetet strävar man efter att få nödvändig utländsk underrättelseinformation till försvarsmaktens förfogande.

Försvarsattachéerna vid utrikesbeskickningarna

Enligt artikel 3 i Wienkonventionen om diplomatiska förbindelser omfattar en diplomatisk beskicknings uppgifter bl.a. att med alla lagliga medel hålla sig underrättad om

förhållandena och utvecklingen i den mottagande staten samt att avge rapporter därom till den sändande statens regering. I artikel 7 i konventionen nämns av beskickningspersonalen särskilt militär-, marin- och flygattachéerna.

Finland har totalt cirka 20 ackrediterade försvarsattachéer i flera stater. De nämna tjänstemännen rapporterar till militärunderrättelsen om sitt stationeringsland. I de lagar som gäller försvarsmakten finns inga bestämmelser om befogenheterna för försvarsmaktens tjänstemän som är verksamma vid beskickningarna.

Militärunderrättelsen som en del av krishanteringsoperationerna

Enligt 2 § 1 mom. 3 punkten i lagen om försvarsmakten är det försvarsmaktens uppgift att delta i internationell militär krishantering. I 2 kapitlet i samma lag föreskrivs om försvarsmaktens befogenheter. Enligt 13 § i lagen deltar försvarsmakten i internationell militär krishantering på det sätt som bestäms i lagen om militär krishantering (211/2006).

Enligt 5 § i lagen om militär krishantering ger försvarsministeriet försvarsmakten de uppdrag som den militära krishanteringen förutsätter samt styr och övervakar den militära krishanteringen. Den finska krishanteringsorganisationen kan omfatta krishanteringsstyrkor, avdelta enheter och enskilda personer. Krishanteringsorgansationen hör till försvarsmakten och är underställd Huvudstaben på det sätt som bestäms i 5 § i lagen om militär krishantering. I operativt hänseende är krishanteringsorganisationen underställd den föranstaltare som avses i 1 § 3 mom. i lagen om militär krishantering. Dessa är FN, Organisationen för säkerhet och samarbete i Europa (Osse), Europeiska unionen (EU), Nordatlantiska alliansen (Nato) eller någon annan internationell organisation eller grupp av länder. Varken i lagen om militär krishantering eller i någon av de lagar som gäller försvarsmaktens verksamhet finns det någon specialreglering av krishanteringsoperationernas militärunderrättelse. I operationerna kan underrättelseorgan ingå.

I en krishanteringsoperation verkar en militär styrka på en annan stats territorium. De militära styrkornas ställning på en annan suverän stats territorium (operationens värdstat) ordnas genom avtal där styrkornas juridiska ställning och immunitet på värdstatens territorium överenskoms. Dessa avtal kallas avtal som reglerar styrkornas juridiska ställning (Status of Forces Agreement, SOFA-avtal). Principen är att för förhandlingarna om SOFA-avtal svarar den som har gett fullmakt till eller verkställer operationen i förhållande till operationens värdstat. I regel inriktas de skyldigheter som följer av dessa avtalsarrangemang, i praktiken beviljandet av privilegier och rättigheter till krishaneringsstyrkan, ensidigt på operationens värdstat. Det är skäl att framhäva att SOFA-avtalen inte skapar några befogenheter för de styrkor som tjänstgör i operationerna. Befogenheterna följer av operationens folkrättsliga mandat, den nationella lagstiftningen i de länder som sänder ut styrkor samt av de militära kommandon som ges i operationen.

3.4 Om bekämpning av hoten mot dataskyddet

3.4.1 Allmänt

I egenskap av ett informationssamhälle och en ekonomi som stöder sig på den internationella marknaden är Finland beroende av att informationsinfrastrukturen fungerar utan störningar. Att kommunikationsnäten och kommunikationstjänsterna fungerar och är tillförlitliga är viktiga förutsättningar för tillväxten i den finska ekonomin, för konkurrenskraften, innovationerna och välfärden inom samhällets alla verksamhetsområden.

Det är viktigt att informationsstrukturen fungerar säkert också med tanke på samhällets övergripande säkerhet. Det att samhället blir allt mera datatekniskt, att det utländska ägandet i datakommunikationsinfrastrukturen ökar samt att statsförvaltningens datatekniska funktioner utlokaliseras ställer krav av nya slag på tryggandet av samhällets vitala funktioner. Med samhällets vitala funktioner avses tväradministrativa funktionshelheter som är vitala för samhället och som måste vara säkerställda i alla situationer. Om de datatekniska systemen inte fungerar, informationsinfrastrukturen kollapsar och olika hot mot dataskyddet visar sig, påverkar detta negativt de offentliga tjänsterna, företagslivet samt förvaltningen och därmed hela samhällets verksamhet. Största delen av Finlands kritiska datakommunikationsinfrastruktur och dess tjänster ägs och produceras av privata sektorn, vilket gör att dess betydelse är stor när det gäller att trygga samhällets vitala funktioner.

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

De parter som använder elektroniska kommunikationsnät och kommunikationstjänster sörjer för sitt dataskydd med olika metoder. Dataskyddet kan upprätthållas t.ex. med dataadministrativa metoder och genom att tekniska begränsningar ställs för användningen av ett kommunikationsnät eller en tjänst. Statsförvaltningens enhetliga natur möjliggör att förvaltningens dataskydd kan styras centraliserat och med stöd av enhetliga principer. Finansministeriet styr och leder det allmänna utvecklandet av den offentliga förvaltningens datasäkerhet och statsförvaltningens datasäkerhet samt ICT-beredskapen. Finansministeriets styrande uppgift grundar sig bl.a. på lagen om styrning av informationsförvaltningen inom den offentliga förvaltningen (634/2011) och lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013).

För att trygga statens högsta lednings beslutsfattande och säkerhetsmyndigheternas lagstadgade uppgifter avlät regeringen år 2013 en proposition med förslag till lag om verksamheten i den offentliga förvaltningens säkerhetsnät (RP 54/2013).[4] Målet är att stifta en lag om ett säkerhetsnät som förenar statens ledning, ministerierna, försvarsmakten, gränsbevakningsväsendet, polisen och räddningsväsendet i samma datakommunikationsnät. Genom säkerhetsnäten kan man försäkra sig om att myndigheterna har beredskap inför datakommunikationsstörningar och att datakommunikationen fortgår.

Den offentliga förvaltningens säkerhetsnät erbjuder alla användare och deras centrala tjänsteproducenter en stabil data- och kommunikationsteknisk tjänstemiljö. Säkerhetsnätets datakommunikations- och dataskyddslösningar gör det möjligt att genomföra olika skyddsnivåer samt gemensamma eller separata databehandlingsomgivningar för användarna. På detta sätt uppnår man kostnadseffektivt ett datanät som är gemensamt för myndigheterna och täcker hela landet och det fungerar tillförlitligt också under undantagsförhållanden och medan bl.a. naturfenomen, elavbrott eller de hela tiden ökande datanätsattackerna pågår. Finansministeriet ska under normala förhållanden och störningssituationer som anknyter till dem besluta om hur förstahands-, akut- och annan viktighetsordning bestäms för säkerhetsnätets tjänsteproduktion och användningen av nätet.

Finansministeriet inledde också under år 2013 ett projekt för att utveckla statens dataskyddsverksamhet dygnet runt (SecICT). Projektet har till uppgift att planera och grunda en myndighetsfunktion för att förebygga och samordna omfattande och allvarliga störningssituationer i dataskyddet. I projektet breddas och utvecklas de tjänster som förbättrar statsförvaltningens datasäkerhet. Dessutom startar inom projektet grupper som får till uppgift att åtgärda störningarna. Utvecklandet görs i samarbete mellan statens och den privata sektorns aktörer inom data- och cybersäkerheten samt med pilotorganisationer. Avsikten är att projektet ska avslutas vid utgången av år 2015, varvid en ny funktion inleds från början av år 2016.

På den privata sektorn är det inte möjligt att ha en centraliserad dataskyddsstyrning, utan nivån på dataskyddet och de lösningar som valts för att upprätthålla dataskyddet varierar enligt varje organisations egna behov och betoningar. Upptäckten av dataskyddshot och skuddandet mot dem baserar sig såväl inom förvaltningen som också på den privata sektorn i praktiken på kommersiella dataskyddsprogram och dataskyddstjänster. En del av statsförvaltningen och de företag som är kritiska med tanke på försörjningsberedskapen utnyttjar i sitt skyddande också Kommunikationsverkets system för upptäckt av och varning för allvarliga dataskyddsintrång (det s.k. HAVARO-systemet, förkortat på finska).

[4] Riksdagen har den 19 december 2014 antagit lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (RSv 245/2014 rd)

3.4.2 Informationssamhällsbalkens 272 §

Informationssamhällsbalken (917/2014) antogs i riksdagen den 15 oktober 2014 (Rsv 106/2014 rd) och den trädde i kraft den 1 januari 2015. Genom lagen upphävdes lagen om dataskydd vid elektronisk kommunikation. I 272 § i informationssamhällsbalken ingår en bestämmelse som har samma innehåll som 20 § i den upphävda lagen. Informationssamhällsbalken har stiftats med grundlagsutskottets medverkan. Informationssamhällsbalkens 272 § ger företag, sammanslutningar och myndigheter som utnyttjar elektroniska kommunikationstjänster i syfte att sörja för informationssäkerheten rätt att analysera innehållet i de meddelanden som kommer till och skickas från nätet bl.a. för att upptäcka, förhindra och utreda störningar som inverkar menligt och göra störningarna till föremål för förundersökning.

I förarbetet till den nu upphävda lagens 20 § (RP 125/2003 rd, s. 76) hänvisas det med uttrycket ”störningar som orsakar skada” bl.a. till omfattande uppsåtlig spridning och användning av skadliga program. I detaljmotiveringen till 272 § i informationssamhällsbalken konstateras det att ändringen inte är avsedd att ändra det rådande rättsläget (RP 221/2013 rd, s. 202).

Automatisk analys av innehållet i kommunikationen gäller innehållet i alla de meddelanden som kommer in i och skickas ut ur datanätet eller datasystemet hos den part som använder sig av automatisk analys. Det huvudsakliga syftet med analyseringen är att upptäcka de skadliga programmens försök att tränga in i datasystemet samt den kommunikation som skadliga program, som eventuellt redan har trängt in i systemet, för med sina värdar.

De skadliga programmen och kommandona identifieras i en första fas vid automatisk analys av innehållet utgående från på förhand fastställda definitioner, och innehållet i meddelandet kommer då inte till den fysiska personens kännedom. Om det är uppenbart att ett meddelande som kommit fram vid automatisk filtrering innehåller ett skadligt program och dataskyddet inte kan säkerställas med automatiska medel, tillåter 272 § i informationssamhällsbalken att företaget, sammanslutningen eller myndigheten tar meddelandets innehåll till behandling manuellt.

3.4.3 Kommunikationsverkets Cybersäkerhetscenter

Kommunikationsverkets Cybersäkerhetscenter är en nationell informationssäkerhetsmyndighet som bl.a. förebygger, samlar information om och reder ut intrång i dataskyddet som anknyter till de allmänna kommunikationsnäten och via dem är riktade mot finska parter samt informerar om betydande hot mot informationssäkerheten. Enligt cybersäkerhetsstrategin har Cybersäkerhetscentret också till uppgift att sammanställa och upprätthålla en lägesbild över cybersäkerheten. Cybersäkerhetscentret samlar in uppgifter om händelser i datanäten och förmedlar dem till olika aktörer samt utformar och delar cybersäkerhetens sammanställda lägesbild. Cybersäkerhetscentrets

kunder kan utnyttja lägesbildsuppgifterna när de organiserar och prioriterar sin beredskap.
Vid formandet av lägesbilden utnyttjas utöver nationella källor också Cybersäkerhetscentrets internationella samarbetsnätverk, som bygger på frivillighet och ömsesidigt förtroende. Moderorganisationerna till de GovCERT-grupper som ingår i samarbetsnätverket är placerade i olika segment inom statsförvaltningen i sina respektive länder. Till exempel Sveriges CERT-SE är en del av ett civilt beredskapsverk medan igen Tysklands CERT-BUND är verksamt inom inrikesministeriets förvaltningsområde. I en del stater har CERT-grupperna placerats inom försvarsministeriets förvaltningsområde och i en del verkar CERT-grupperna igen som en del av underrättelsemyndigheten (Government Communications Headquarters, GCHQ).

HAVARO är ett system för upptäckt av och varning om intrång i dataskyddet som Kommunikationsverkets Cybersäkerhetscenter erbjuder företag och statsförvaltningens aktörer, vilkas verksamhet är av största vikt med tanke på försörjningsberedskapen. Verksamheten grundar sig på 272 § i informationssamhällsbalken (tidigare 20 § i den lag som upphävdes). Syftet med HAVARO-systemet är att med olika identifierare identifiera skadlig nättrafik och utvecklade nätattacker som äventyrar dataskyddet (Advanced Persistent Threat, APT). Ett andra syfte med systemet är att stöda formandet av en bättre lägesbild av de dataskyddshot som riktar sig mot finska datanät. De tekniska identifierare av skadliga program som ska utnyttjas i systemet grundar sig huvudsakligen på information som Cybersäkerhetscentret fått av inhemska och utländska samarbetspartner.

4 INTERNATIONELL JÄMFÖRELSE

Detta kapitel behandlar lagstiftningen i Sverige, Norge, Danmark, Nederländerna och Tyskland med anknytning till den försvarsunderrättelse som gäller hot som riktar sig mot den nationella säkerheten generellt och den signalspaning som görs i datanätsomgivningen mera specifikt.

4.1 Sverige

4.1.1 Allmän reglering av försvarsunderrättelseverksamheten

Bestämmelser om försvarsunderrättelseverksamheten finns i den allmänna lagen om försvarsunderrättelseverksamhet och i en förordning som kompletterar den samt i speciallagar.[5] Försvarsunderrättelseverksamhet bedrivs av Försvarsmakten, Försvarets radioanstalt FRA, Försvarets materielverk FMV och Totalförsvarets forskningsinstitut

[5] Lag (2000:130) om försvarsunderrättelseverksamhet, Förordning (2000:131) om försvarsunderrättelseverksamhet, Lag (2007:258) om behandling av personuppgifter i försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Förordning (2007:260) om behandling av personuppgifter i försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

FOI som är underställt Försvarsdepartementet. Området för underrättelse har avgränsats så att underrättelseverksamhet bedrivs till stöd för svensk utrikes-, säkerhets- och försvarspolitik och för att kartlägga yttre hot mot landet. Försvarsunderrättelseverksamhet får endast gälla utländska förhållanden.

Regeringen bestämmer försvarsunderrättelseverksamhetens inriktning. Inom ramen för denna inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten. Underrättelsesverksamheten fullgörs genom inhämtning, bearbetning och analys av information. I verksamheten används teknisk och personbaserad inhämtning från både öppna och andra källor. Underrättelserna rapporteras till de parter som gett uppdraget samt till övriga eventuella berörda parter. Den eller de myndigheter som ska bedriva försvarsunderrättelseverksamhet får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer.

Inom försvarsunderrättelseverksamheten får det inte vidtas åtgärder som syftar till att lösa uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens, säkerhetspolisens eller andra lagövervakningsmyndigheters brottsbekämpnings- eller förebyggandebefogenheter.[6] Enligt förarbetet[7] till lagen om försvarsunderrättelseverksamhet avses med detta att i underrättelseverksamheten inte genom kringgående av annan lagstiftning får användas sådana förundersöknings- eller tvångsmedelsbefogenheter, om vilkas användningsområde och förutsättningar för användning föreskrivs i rättegångsbalken och t.ex. i polislagen. Å andra sidan får vid underrättelseverksamhet stöd ges brottsbekämpningsmyndigheterna. Till denna del konstateras i förarbetet till lagen[8] att säkerhetspolisen i dagens läge till många delar har formen av en underrättelsetjänst och även riktar in sig på att inhämta information som gäller verksamhet som bedrivs utomlands men äventyrar Sveriges säkerhet. Inom ramen för denna uppgift måste säkerhetspolisen kunna utnyttja också den informationsinhämtningskapacitet som de myndigheter har som svarar för underrättelseverksamheten.

De myndigheter som bedriver underrättelseverksamhet är skyldiga att rapportera till Försvarsdepartementet om verksamhetens allmänna inriktning, internationellt samarbete samt om den underrättelseverksamhet som ska bedrivas med särskilda metoder för informationsinhämtning. Dessa särskilda metoder för informationsinhämtning har det ansetts att inte kan specificeras i lagen, men i förarbetet till lagen konstateras att med dem hänvisas det huvudsakligen till person- och signalspaning.[9] Underrättelsemyndigheterna ska också årligen göra en offentlig allmän översikt över det gångna årets underrättelseverksamhet. Statens inspektion för försvarsunderrättelseverksamhet (SIUN), som har tillsatts av regeringen, övervakar försvarsunderrättelseverksamheten.

[6] Ändring av bestämmelsen trädde i kraft 1.1.2015. Tidigare formulering: ”- - polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet.”
[7] Regeringens proposition 1999/2000:25
[8] Regeringens proposition 2006/07:63: ”En anpassad försvarsunderrättelseverksamhet”.
[9] Regeringens proposition 2006/07:63: ”En anpassad försvarsunderrättelseverksamhet.”

SIUN övervakar bl.a. att lagen följs, inriktningen av underrättelsen och de metoder som används vid inhämtningen av information.

4.1.2 Signalspaning

Bestämmelser om signalspaning finns i speciallagar och en specialförordning om detta.[10] Signalspaning idkas av Försvarets radioanstalt (FRA), som är en civil organisation underställd försvarsdepartementet, och därmed inte en del av försvarsmakten. FRA har till uppgift att inhämta underrättelseinformation i enlighet med de uppdrag organisationen fått och ställa den inhämtade informationen till uppdragsgivarnas förfogande.

Enligt signalspaningslagen avses med signalspaning att inhämta signaler i elektronisk form. Definitionen är teknikneutral och täcker alla metoder av signalspaning, såsom t.ex. kabel- och radiosignalspaning samt manuell och automatisk informationsinsamling. Signalspaningen delas in i fyra faser, som är inriktning av signalspaningen, insamling av information, bearbetning av informationen och rapportering av den.
En förutsättning för signalspaningen är att de förutsättningar som fastslås både i den allmänna försvarsunderrättelselagen och i speciallagen om signalspaning uppfylls. Enligt den allmänna lagen ska det vara fråga om försvarsunderrättelseverksamhet som bedrivs till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt för kartläggning av yttre hot mot landet. Speciallagen om signalspaning definierar för sin del uttömmande vilka hot och situationer signalspaning får användas för att kartlägga.[11] Om det är nödvändigt för verksamheten, kan information inhämtas också för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt för att utveckla den teknik och metodik som behövs för att bedriva verksamheten. En allmän avgränsning är att om både mottagaren och avsändaren av signaler befinner sig i Sverige, får signalerna inte inhämtas.

För att signalspaning ska få bedrivas förutsätts alltid ett uppdrag, som Regeringen, Regeringskansliet, Försvarsmakten, Rikskriminalpolisen eller Säkerhetspolisen kan ge FRA. Uppdraget får inte avse endast en viss fysisk person.
Även om lagen är teknikneutral, ingår det i den några specialbestämmelser som gäller signalspaning i trådar. Spaningen får gälla datatrafiken längs trådar, endast när den överskrider Sveriges gräns.

Signalspaning förutsätter alltid tillstånd av försvarsunderrättelsedomstolen, som är en specialdomstol. Ansökan om tillstånd som gäller signalspaning i trådar ska innehålla

[10] Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet, Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet och Förordning (2008:923) om signalspaning i försvarsunderrättelseverksamhet.
[11] Sådana situationer är enligt 1 § i lagen om signalspaning: a) yttre militära hot mot landet, b) svenska intressen i internationella insatser, c) internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota nationella intressen, d) massförstörelsevapen, e) allvarliga yttre hot mot samhällets infrastrukturer, f) konflikter utomlands med konsekvenser för internationell säkerhet, g) främmande underrättelseverksamhet mot svenska intressen eller h) främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

en redogörelse för spaningsuppdraget, uppgift om vilken eller vilka signalbärare avseende signaler i tråd man vill inrikta spaningen på, de sökbegrepp som ska användas, vilken tid tillståndet ska gälla och de omständigheter i övrigt som signalspaningsmyndigheten vill åberopa. I lagen har också ställts exakta förutsättningar för när domstolen får bevilja tillstånd och vad som ska framgå av tillståndet. Förutsättningarna för beviljande sammanhänger i synnerhet med verksamhetens och uppdragets lagenlighet och proportionalitet. Av tillståndet ska framgå inhämtningsuppdraget, vilken eller vilka signalbärare avseende signaler i tråd tillståndet gäller, vilka sökbegrepp eller kategorier av sökbegrepp som får användas, den tid som tillståndet avser och de villkor i övrigt som behövs för att begränsa intrånget i enskildas personliga integritet. Med sökbegrepp avses enligt förarbetet till lagen[12] sådana begrepp med hjälp av vilka i en informationsmängd kan hittas sådana poster eller uppgiftskonstellationer där begreppet i fråga förekommer. Sökbegreppet kan också innehålla sådana variabler med vilka man kan särskilja mellan större informationsmängder.

Möjligheten att använda ett sökbegrepp som hänvisar till en enskild fysisk person har begränsats för att integritetsskyddet ska kunna säkerställas. Ett sådant sökbegrepp kan användas endast om det är särskilt viktigt med tanke på underrättelseverksamheten. Dessutom har FRA en skyldighet att ge en redogörelse om dylika sökbegrepp till Statens inspektion för försvarsunderrättelseverksamhet som övervakar signalspaningen. En fysisk person ska underrättas så snart som möjligt och senast en månad efter att spaningsuppdraget har avslutats om när och i vilket syfte spaningen har genomförts, om inget annat följer av sekretessbestämmelserna.

Informationsinsamling i datakommunikationstrådar förutsätter samarbete med datakommunikationsoperatören. Till följd av detta är de datakommunikationsoperatörer som äger tråd i vilka signaler förs över Sveriges gräns skyldiga att överföra dessa till samverkanspunkter. Dessutom är operatörerna skyldiga att till myndigheten lämna sådan information som gör det enklare att ta hand om signalerna. Operatörerna bör vidta ovan nämnda åtgärder så att verksamheten inte röjs.[13]

Endast övervakningsmyndigheten Statens inspektion för försvarsunderrättelseverksamhet har tillträde till den datakommunikation som operatörerna har fört till samverkanspunkterna. Myndigheten har till uppgift att avskilja och ge FRA tillträde endast till de signalbärare som har specificerats i domstolens tillstånd.[14] De sökningar som FRA gör riktas mot dessa trådar. FRA rapporterar till uppdragsgivaren om den information som organisationen inhämtat genom signalspaningen samt under de förutsättningar som fastslås i lagen också till andra myndigheter.

[12] Regeringens proposition 2006/07:63, s. 76-77.
[13] Lag (2003:389) om elektronisk kommunikation 6 kap. 19 a §
[14] Lagen om signalspaning 12 §. Det är fråga om en ändring som gjorts genom lag 2009:967 för vilken gäller regeringens proposition 2008/09:21 Förstärkt integritetsskydd vid signalspaning. Tidigare var det FRA som genomförde informationsinhämtningen i samverkanspunkten enligt tillståndsvillkoret. Ändringen motiverades med att signalspaningens trovärdighet ökar om singlaspaningsmyndigheten inte har tillträde till andra signalbärare än dem som tillståndet gäller.

Vid FRA finns ett integritetsskyddsråd, som har till uppgift att övervaka att integritetsskyddet förverkligas. Rådet rapporterar till FRA:s ledning och vid behov till Statens inspektion för försvarsunderrättelseverksamhet. Vidare övervakas signalspaningen också av dataombudsmannen, riksdagens justitieombudsman och justitiekansler. Den övervakning som Statens inspektion för försvarsunderrättelseverksamhet utför gäller framför allt användningen av signalspaningens sökbegrepp, förstörandet av och rapportering om uppgifterna. Den kan också bestämma att en spaningsåtgärd ska avslutas och uppgifterna förstöras, ifall verksamheten inte har följt tillståndet. Statens inspektion för försvarsunderrättelseverksamhet kan på begäran av en fysisk person granska, om dennes meddelanden har följts och om det eventuella följandet har varit förenligt med lagen. Datainspektionen övervakar att integritetsskyddet realiseras också i FRA:s verksamhet.

Bestämmelser om behandlingen av personuppgifter som inhämtats med signalspaning finns i en särskild lag.[15]

4.2 Norge

Bestämmelser om Norges underrättelse och underrättelsetjänstens verksamhet finns i lagen om underrättelsetjänsten och den preciseras i en förordning.[16] Försvarsdepartementet kan utfärda bestämmelser som kompletterar förordningen. Underrättelseverksamhet utövas av Norges underrättelsetjänst *(Etterretningstjenesten, E-tjenesten, NIS)* som finns inom försvarsmaktens organisation. Den svarar i enlighet med lagen om underrättelsetjänsten för att upptäcka och analysera yttre hot samt utländska aktörers motiv, deras prestationsförmåga och de metoder de använder. Syftet med underrättelseverksamheten är att förhindra hot och skapa en hållbar grund för det beslutsfattande som gäller utrikes-, säkerhets- och försvarspolitiken. För styrningen och övervakningen svarar försvarsdepartementet som underrättelsetjänsten har rapporteringsskyldighet till i fråga om sin verksamhet. För statens interna säkerhet svarar polisens säkerhetstjänst *(Politiets sikkerhetstjeneste, PST)*.

Norges underrättelsetjänst har till uppgift att inhämta, bearbeta och analysera information som gäller norska intressen i relation till främmande stater, organisationer och individer och mot denna bakgrund utarbeta analyser av hoten och underrättelsebedömningar i den omfattning som detta kan medverka till att viktiga nationella intressen tryggas.[17] Den lista på nationella intressen som ingår i lagen är emellertid inte uttömmande. Försvarsdepartementet ger underrättelsetjänsten uppdragen via chefen för

[15] Lag (2007/259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.
[16] Lov om etterretningstjenesten 1998-03-20 nr 11 och Instruks om etterretningstjenesten FOR 2001-08-31 nr 1012.
[17] Sådana viktiga nationella intressen är bl.a. a) utformning av Norges utrikes-, försvars- och säkerhetspolitik, b) beredskapsplanering och krishantering, c) försvarsmaktens planering på lång sikt och strukturutveckling, d) försvarsmaktens operativa avdelningars effektivitet, e) stöd till sådana försvarsallianser där Norge är med, f) norska styrkor som är med i internationella militära insatser, g) Norges deltagande i internationella nedrustnings- och vapenbegränsningsavtal och bevakning av dessa avtal samt h) internationell terrorism, i) globala miljöproblem, j) spridningen av massförstörelsevapen och de anordningar och det material som behövs för tillverkning av sådana vapen.

försvarsmakten. Underrättelsetjänsten ska utarbeta utredningar och samla in information enligt regeringens och vederbörande departements behov. Underrättelsetjänsten har en föreskriven rätt till internationellt underrättelsesamarbete med andra länder och internationella organisationer samt en särskild skyldighet att idka samarbete med de försvarsallianser som Norge hör till.

Det finns inget föreskrivet om de metoder för inhämtning av information som underrättelsetjänsten har till sitt förfogande. Informationsinhämtningen har dock begränsats i lag på så sätt att underrättelsetjänsten inte inom norskt territorium får övervaka och inte annars heller i hemlighet samla in information om norska fysiska eller juridiska personer. Som ett undantag till detta kan underrättelsetjänsten emellertid samla in information om sådana norska personer som deltar i olovlig underrättelseverksamhet för en främmande stats räkning. Då måste informationsinhämtningen ske genom förmedling av polisens säkerhetstjänst eller med godkännande av den.

Samarbetet mellan underrättelsetjänsten och polisens säkerhetstjänst regleras i en förordning[18], med vilken avsikten är att främja samarbetet mellan parterna. Prioriterade sektorer för samarbetet är bekämpning av terrorism, av spridningen av massförstörelsevapen och av olovlig underrättelseverksamhet samt andra förhållanden som gäller viktiga norska intressen. Tjänsterna ska bistå varandra såväl i genomförandet av konkreta informationsinhämtningsinsatser och utbyte av operativ information som också vid analyseringen av strategiska uppgifter och hotbedömningar. En förutsättning för samarbetet är att parterna följer de bestämmelser som utfärdats om deras befogenheter.

Bestämmelser om övervakningen av underrättelsetjänsten ingår i lagen om övervakning av underrättelse-, övervaknings- och säkerhetstjänsterna, som är gemensam för alla säkerhetsmyndigheter.[19] Enligt lagen övervakas underrättelsetjänsten av stortingets övervakningsutskott för underrättelse-, övervaknings- och säkerhetstjänster. Utskottet är självständigt och oberoende av stortinget i sin verksamhet. Syftet med övervakningen är att förhindra och reda ut eventuella missbruk, försäkra sig om att de metoder som används i underrättelsen står i rätt proportion och att de mänskliga rättigheterna respekteras samt övervaka att verksamheten är lagenlig och inte orsakar samhället oskälig skada. Övervakningen görs både på eget initiativ och genom att klagomål behandlas. Utskottet har inom ramen för dess uppgifter garanterats vidsträckta rättigheter att få tillträde till underrättelsetjänstens arkiv, register och lokaler. Övervakningsutskottet ger årligen en rapport över sin verksamhet till stortinget.

4.3 Danmark

I Danmark bedrivs underrättelse av Försvarets underrättelsetjänst *(Forsvarets Efterretningstjeneste, FE)* som är en civil myndighet, underställd försvarsministeriet. I la-

[18] Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste 13. oktober 2006 nr 1151.
[19] Lov om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste 1995-02-03 nr 07.

gen om försvarsmaktens underrättelsetjänst föreskrivs om dess uppgifter, behörighet och övervakningen av underrättelseverksamheten.

FE svarar för både Danmarks utlandsunderrättelse och militärunderrättelse. FE är också nationell dataskyddsmyndighet. FE:s uppgifter och verksamhet regleras genom lagen om Försvarets underrättelsetjänst från år 2013[20], som ersatte den synnerligen snäva reglering som tidigare ingick i den s.k. försvarslagen[21]. Lagstadgade uppgifter för FE är att skapa en underrättelsegrund för Danmarks utrikes-, säkerhets- och försvarspolitik, hjälpa till att förhindra och avvärja hot som riktar sig mot Danmark och danska intressen, och i dessa syften samla in, bearbeta och analysera information som gäller utländska relationer, vilka är av betydelse för Danmark och danska intressen utomlands samt rapportera om dem. FE har en skyldighet att informera försvarsministeriet om förhållanden som har betydelse för Danmark och dess intressen, samt om omständigheter och faktorer som har påverkan på FE:s uppgiftsfält. Genom beslut av försvarsministern kan underrättelsetjänsten dessutom utföra andra uppgifter som hänför sig till någon av underrättelsetjänstens uppgifter som nämns ovan.

Regleringen av FE:s befogenheter är generell. FE får samla in och inhämta information, som kan ha betydelse för den underrättelseverksamhet den bedriver. När FE sköter informationsinhämtningsuppdrag som riktar sig mot förhållanden utomlands får den också samla in information om danska medborgare och danska juridiska personer samt om utlänningar som vistas i landet. Mera exakt än detta har i lagen inte föreskrivits om underrättelsetjänstens befogenheter och lagen specificerar inte de olika sätten att inhämta information. Enligt offentliga källor görs inhämtningen av information såväl i form av inhämtning av information om personer, elektroniskt via satelliter och datakommunikationslinjer på marken med hjälp av signalspaning som också från öppna källor.[22] På behandlingen av personuppgifter tillämpas både i fråga om fysiska och juridiska personer bestämmelserna i lagen om behandling av personuppgifter i tillämpliga delar. I lagen ingår inga bestämmelser om tillståndsförfarandet gällande informationsinhämtning.

Vid sidan av underrättelsetjänsten finns i Danmark polisens säkerhetstjänst *(Politiets Efterretningstjeneste, PET)*. Det finns inga uttryckliga bestämmelser om PET:s utlandsverksamhet, men enligt förarbetet till den lag[23] som reglerar dess verksamhet anses PET ha rätt att genomföra gemensamma informationskällsinsatser tillsammans med underrättelsetjänsten och utländska underrättelseorgan såväl i Danmark som utomlands. Informationskällor kan också sändas utomlands för att samla in information som hör till PET:s verksamhetsområde.

[20] Lov om Forsvarets Efterretningstjeneste (602/2013).
[21] Lov om forsvarets formål, opgaver og organisation m.v. (122/2011).
[22] http://fe-ddis.dk besök 8.12.2014.
[23] Lov om Politiets Efterretningstjeneste

FE och PET får överlåta personuppgifter och andra uppgifter till varandra, om överlåtandet kan ha betydelse för utförandet av deras uppdrag. Syftet är att parterna inte i samband med varje enskilt överlåtande av information ska bli tvungna att separat bedöma, om överlåtandet är nödvändigt. Enligt det statliga betänkande där det föreslogs att lagarna om FE och PET skulle stiftas är de båda tjänsternas uppgifter så nära förbundna med varandra att överlåtelse av uppgifter mellan dem i stor utsträckning ska jämställas med överlåtelse av uppgifter inom en myndighet.[24]

FE:s verksamhet övervakas av försvarsministeriet, en övervakningskommitté, folktingets underrättelsetjänsteutskott samt i fråga om användningen av penningmedel av statsekonomins revisionsverk.
Övervakningskommitténs centrala uppgift är att övervaka att underrättelse- och säkerhetstjänsternas behandling och registrering av personuppgifter stämmer överens med lagen. Kommittén kan ta ett ärende, som gäller behandlingen av personuppgifter, till undersökning antingen på eget initiativ eller på begäran av den registrerade. Kommittén kan också utföra granskningar och inspektioner i underrättelse- och säkerhetstjänsternas lokaler och den har allmän rätt att få information om deras personregister och tjänstemän. Kommittén kan ge utlåtanden och rekommendationer till underrättelsetjänsterna.

Folktingets underrättelsetjänsteutskott är ett gemensamt parlamentariskt specialövervakningsorgan för underrättelse- och säkerhetstjänsterna. Regeringen ska informera utskottet om de riktlinjer som den har dragit upp för underrättelse- och säkerhetstjänsternas verksamhet samt om sådana frågor med anknytning till säkerheten eller utrikespolitikens område som har betydelse med tanke på deras verksamhet. För att väsentliga nya uppgifter ska kunna ges underrättelse- och säkerhetstjänsterna förutsätts att uppgifterna först har behandlats i utskottet.

4.4 Nederländerna

4.4.1 Underrättelse- och säkerhetstjänsterna

I Nederländerna bedrivs underrättelseverksamhet av Allmänna underrättelse- och säkerhetstjänsten *(Algemene Inlichtingen- en Veiligheidsdienst, AIVD)*, som är underställd inrikesministeriet, och militärunderrättelse- och säkerhetstjänsten *(Militaire inlichtingen en veiligheid, MIVD)*, som är underställd försvarsministeriet. Bestämmelser om bådas uppgifter och befogenheter finns i lagen om underrättelse- och säkerhetstjänster.[25] Den behöriga ministern har dessutom rätt att utfärda en mera detaljerad reglering av det underlydande organets organisation, arbetssätt och ledning.

[24] Betaenkning om PET og FE (1529/2012).
[25] Wet op de inlichtingen- en veiligheidsdiensten 2002, Intelligence and Security Services Act, ISSA 2002 (eng.).

AIVD och MIVD utför både underrättelse och kontraunderrättelse. Tjänsterna är skyldiga att stödja varandra vid utförandet av uppgifterna. De har en gemensam koordinator, vars uppgift det är att sörja för att förfaringssätten samordnas. Cheferna för underrättelse- och säkerhetstjänsterna är skyldiga att stödja koordinatorn i hens uppgift.

För upprätthållandet av den nationella säkerheten har Allmänna underrättelse- och säkerhetstjänsten till uppgift att inhämta information om och bedöma grupper, personer och främmande stater som äventyrar den demokratiska samhällsordningen eller statens vitala intressen, att främja åtgärder för att skydda statens vitala intressen samt att utarbeta hot- och riskbedömningar för att skydda vissa personer, tjänster och viss egendom.

För upprätthållandet av den nationella säkerheten har Militärunderrättelse- och säkerhetstjänsten till uppgift att inhämta information om och bedöma den operativa prestationsförmågan hos andra staters vapenmakter, göra säkerhetsutredningar, undersöka och bedöma tillståndet hos och organiseringen av den egna vapenmakten, främja skyddandet av vapenmaktens operativa intressen samt utarbeta hot- och riskbedömningar för skyddande av militära objekt och vissa personer, lokaler och tjänster i anknytning till dem.

I Nederländerna är befogenhetsregleringen synnerligen detaljerad. Säkerhets- och underrättelsetjänsterna bör i första hand använda information som finns i offentliga källor eller kan erhållas från samarbetspartner. Utöver detta har de rätt att använda särskilda befogenheter som definieras i lag och med stöd av vilka de kan bedriva t.ex. person- och signalspaning.[26] För att de särskilda befogenheterna ska få användas förutsätts tillstånd, som i regel beviljas av inrikesministern eller försvarsministern. Bland andra principen om minsta olägenhet och proportionalitetsprincipen gäller användningen av befogenheterna.

Underrättelse- och säkerhetstjänsterna rapporterar årligen om sin verksamhet till parlamentet. Den rapport som de styrande ministrarna ger innehåller en översikt över hurdana objekt tjänsterna har inriktat eller kommer att inrikta sin verksamhet på.

En oberoende bedömningskommitté bedömer om underrättelse- och säkerhetstjänsternas verksamhet är lagenlig. Kommittén tillsattes för att säkerställa integritetsskyddet enligt artikel 8 och den rätt som gäller ett effektivt rättsmedel enligt artikel 13 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Övervakningskommittén behandlar och undersöker klagomål som anförts över underrättelse- och säkerhetstjänsternas verksamhet. Övervakningskommittén ger ett förslag till lösning på klagomålet till den ansvariga ministern. Förslaget binder inte

[26] De befogenheter om vilka föreskrivs i lagen om underrättelse- och säkerhetstjänster gäller bl.a. observation, teknisk observation, täckoperationer, grundande av täckorganisationer, styrd användning av informationskällor, hemliga efterspaningar, hemligt öppnande av postförsändelser samt intrång i datatekniska omgivningar t.ex. genom att krypteringen hävs och teleavlyssning.

ministern. Om klagomålsställaren är missnöjd med det avgörande som ministern fattat i saken, kan det överklagas till justitieombudsmannen. Utöver laglighetsövervakning har övervakningskommittén till uppgift att ge råd och rekommendationer gällande underrättelse- och säkerhetstjänsterna till de ministrar som är ansvariga för verksamheten.

Kommittén kan utföra granskningar och inspektioner i underrättelse- och säkerhetstjänsternas lokaler. I anknytning till sina uppgifter har den allmän rätt att få information.

Utskottet för underrättelse- och säkerhetstjänster i parlamentets underhus är ett parlamentariskt specialövervakningsorgan som övervakar underrättelse- och säkerhetstjänsterna. Utskottet rapporterar om sitt arbete till parlamentet.

4.4.2 Utvecklandet av lagstiftningen

Behoven att revidera lagen om underrättelse- och säkerhetstjänster har behandlats i ett betänkande som den s.k. Dessens-kommittén[27] avlät den 2 december 2013. Enligt betänkandet är lagen i för hög grad teknikbunden, vilket gör att utvecklingen inom kommunikationstekniken har gjort den föråldrad. Gällande lag förhindrar underrättelsetjänsterna att inrikta effektiv övervakning på datakommunikation som förmedlas via trådförbindelser.

Kommittén föreslår mycket mera omfattande befogenheter än de nuvarande för underrättelse- och säkerhetstjänsterna att bedriva underrättelse i fråga om datakommunikation i tråd. I Dessens betänkande behandlas inte sättet att genomföra underrättelsen, men det skulle uppenbarligen vara fråga om underrättelseverksamhet som grundar sig på signaler i datakommunikationen av samma slag som i Sverige. Som motvikt till den breddning av underrättelsebefogenheterna som kommittén föreslår, anser den att övervakningen av dessa befogenheter bör utvecklas.

Inrikesministeriet och försvarsministeriet har vidtagit åtgärder för att genomföra de rekommendationer gällande underrättelse i datakommunikation som ingår i Dessens betänkande.

4.5 Tyskland

I Tyskland finns tre organ som utför underrättelse på förbundsstatsnivå: allmänna utlandsunderrättelsetjänsten *(Bundesnachrichtendienst, BND)*, militära säkerhetstjänsten *(Militärischer Abschirmdienst, MAD)* och allmänna säkerhetstjänsten *(Bundesamt für Verfassungsschutz, BfV)*. BND svarar för både civil och militär underrättelse medan igen MAD och BfV svarar för kontraunderrättelsen på sina verksamhetsområden. Be-

[27] Evalutiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2002.

stämmelser om BND:s och MAD:s uppgifter och befogenheter finns i lagarna om dem.[28] Bestämmelser om BfV:s och delstaternas allmänna säkerhetstjänsters verksamhet finns i lagen om förbundsstatens grundlagsskydd[29]. Den allmänna reglering av underrättelseverksamheten som ingår i denna lag gäller också BND:s och MAD:s verksamhet.

BND är underställd förbundskanslerns kansli och rapporterar till det om sin verksamhet. BND har till uppgift att samla in och analysera sådan information om utlandet som kan ha betydelse för Tysklands utrikes- och säkerhetspolitik. BND får samla in, behandla och använda den information som är nödvändig vid underrättelse som riktas mot utlandet, inklusive personuppgifter, om inte behandlingen av uppgifterna strider mot bestämmelserna i dataskyddslagen eller i någon annan specialreglering. BND kan utnyttja de underrättelsemetoder som står till dess förfogande, om den information som behövs inte kan erhållas på annat sätt och någon annan myndighet inte är ansvarig för att informationen samlas in.

BND får i sin verksamhet använda metoder, utrustning och anordningar för hemlig informationsinhämtning, ifall detta är nödvändigt för att utföra uppgifterna. Om behandlingen av personuppgifter och om vederbörandes rätt att få information föreskrivs närmare i lagen om grundlagsskydd.

I lagen om begränsning av brev-, post- och telefonhemligheten (G 10-lagen)[30] föreskrivs om BND:s, MAD:s och BfV:s rätt att övervaka och spara telekommunikation samt öppna och granska brev- och postförsändelser. Lagen innehåller bestämmelser om begränsningar i de grundläggande rättigheterna enligt artikel 10 i Tysklands grundlag[31], om förutsättningarna för begränsningarna samt om begränsningsförfarandet, om skydd för privatlivets kärnområde samt om överlåtelse av personuppgifter. Utöver detta föreskrivs i lagen om övervakningen av underrättelseverksamheten.
I G 10 -lagen föreskrivs också särskilt om BND:s rätt att inhämta information om internationell datakommunikation. Informationsinhämtningen måste vara nödvändig och för den ska tillstånd sökas. Huruvida tillstånd beviljas besluts av förbundsstatens minister i samarbete med den G 10 -kommission som behandlas nedan. De automatiska sökbegrepp som ska användas i underrättelse som inriktas på internationella datakommunikationsförbindelser ska vara fastställda både i tillståndsansökan och i tillståndet. Sökbegreppen kan anknyta endast till utredning av de hot[32] som särskilt räk-

[28] Gesetz über den Bundesnachrichtendienst, BND-lagen, BNDG och Gesetz über den militärischen Abschirmdienst, MAD-lagen, MADG.
[29] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, Bundesverfassungsschutzgesetz, BVerfSchG.
[30] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses.
[31] Brev-, post och telefonhemligheten.
[32] Informationssökning som begränsar de grundläggande rättigheterna är enligt 5 § i G 10 -lagen tillåten endast om informationen är nödvändig för att identifiera följande hot: a) en väpnad attack som riktas mot Tyskland, b) ett internationellt terrordåd som omedelbart anknyter till Tyskland, c) internationell spridning av militärvapen samt olaglig utrikeshandel med vapen, databehandlingsprogram och teknologi av ansenlig betydelse, d) sådan narkotikaimport till EU-området som organiseras av professionell eller organiserad brottslighet och som har stor betydelse för Tyskland, e)

nas upp i lagen. Underrättelse- och säkerhetstjänsterna får med stöd av lagen inrikta högst 20 procent av signalbärarspaningen på internationell datakommunikation. Vid personbaserad underrättelseinhämtning får underrättelse- och säkerhetstjänsterna inhämta information från personkällor och styra dessa samt använda felaktiga personuppgifter och vilseledande registeranteckningar.

De centralaste övervakningsorganen är den parlamentariska övervakningsnämnden[33] och G 10 -kommissionen. Andra övervakande parter är dataombudsmannen och förbundskanslerns kansli som övervakar BND.

Parlamentariska övervakningsnämnden övervakar verksamheten hos alla tre myndigheter som utför underrättelse till den del som det inte är fråga om sådana situationer som direkt avses i G 10 -lagen. Inom ramen för sina uppgifter har nämnden en allmän rätt att få information samt rätt att utföra granskningar och inspektioner i underrättelse- och säkerhetstjänsternas lokaler. Övervakningsnämnden ger med jämna mellanrum en rapport om sin verksamhet till förbundsriksdagen.

G 10 -kommissionen övervakar begränsningen av kommunikationshemligheten. Kommissionen beslutar på tjänstens vägnar eller utgående från klagomål om hur lovliga och nödvändiga begränsningarna av artikel 10 i grundlagen är. Kommissionens övervakning inriktas på underrättelsemyndigheternas behandling av personuppgifter samt på hur detta har meddelats vederbörande. Kommissionen har inom ramen för sina uppgifter en allmän rätt att få information samt rätt att göra granskningar och inspektioner i underrättelse- och säkerhetstjänsternas lokaler.

Dataombudsmannen övervakar tillämpningen av dataskyddslagstiftningen.

5 BEDÖMNING AV NULÄGET

De myndigheter som svarar för den nationella säkerheten har till uppgift att genom sin verksamhet förutse och förebygga sådana skadliga gärningar och åtgärder som kan äventyra nationella intressen som uppfattas som särskilt viktiga. Mot Finland kan riktas allvarliga säkerhetshot från utlandet. Utvecklingen i datanäten har minskat betydelsen av fysiskt avstånd när det gäller att realisera hot.

De myndigheter som svarar för den nationella säkerheten bedriver sådan underrättelse som skötseln av deras lagstadgade uppgifter förutsätter. Det finns emellertid inga i lag föreskrivna befogenheter för underrättelse. Underrättelsen baserar sig enbart på den information som kan erhållas ur offentliga källor samt genom internationellt och annat frivilligt samarbete.

---

destabilisering av eurons värde som sker från utlandet, f) internationellt organiserad penningtvätt av ansenlig betydelse eller g) smuggling av utländska personer till EU-området som organiseras av professionell eller organiserad brottslighet.

[33] Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes.

5.1 Den elektroniska kommunikationsteknologin och de hot som riktas mot den nationella säkerheten

På det sätt som framgår av kapitel 2 i betänkandet har utvecklingen av data- och kommunikationsteknologin betydelse av två slag med tanke på hur de hot som riktas mot den nationella säkerheten formas.

Datanäten utnyttjas som ett medel för att kommunicera om sådana planer och avsikter som gäller gärningar som ska utföras i den reella världen. I ett sådant fall utnyttjas datanäten inte som ett medel med vilket dådet utförs, utan som ett medel för planering och förberedelser. Dåden kan till sin art vara militära (väpnad attack) eller också kan de riktas mot andra nationella intressen än statens territoriella integritet (spionage, terrordåd, export av produkter med dubbla användningsområden).

Å andra sidan utnyttjas datanäten som ett egentligt medel för att utföra ett dåd för att på ett mål – t.ex. finska staten – rikta gärningar som allvarligt skadar det. Det kan t.ex. vara fråga om sådana militära cyberoperationer som avses i strategin för cybersäkerheten i Finland, dvs. gärningar som ska karaktäriseras som cyberspionage eller cyberterrorism.

En förutsättning för att genomförandet av dåd som äventyrar den nationella säkerheten ska kunna förhindras är att datanätshot och den kommunikation som gäller hot upptäcks, de parter som står bakom dem identifieras och hotets art reds ut. Den part som ansvarar för bekämpningen måste på ett så tidigt stadium som möjligt få information om hoten och om kommunikation om dem.

5.2 Organisationernas möjligheter att upptäcka de datanätshot som riktas mot dem

De företag, sammanslutningar och myndigheter som använder datanäten skyddar sig mot datanätshot med hjälp av dataskydd. Om rätten att vidta åtgärder för att sörja för informationssäkerheten föreskrivs i 272 § i informationssamhällsbalken. Bestämmelsen ger företag, sammanslutningar och myndigheter verktyg för att upptäcka och avvärja cybergärningar som riktar sig mot dem. Åtgärderna för upptäckande vidtas decentraliserat, varvid deras kvalitet och nivå varierar från organisation till organisation. Informationssamhällsbalkens 272 § och 20 § i dess föregångare lagen om dataskydd vid elektronisk kommunikation har möjliggjort att också ett centraliserat system för upptäckande av hot mot dataskyddet (HAVARO-systemet) har kunnat utvecklas för att skydda de parter som är av betydelse för samhällets övergripande säkerhet.
Av de skadliga programmen är de som det är svårast att upptäcka och som samtidigt orsakar den största skadan på den nationella säkerheten statliga spionprogram och andra skadliga program. De identifikationer som gäller sådana skadliga program är

sådan information med hög skyddsnivå, som i typiska fall byts som en del av säkerhets- och underrättelsetjänsternas internationella samarbete. Eftersom Kommunikationsverket varken är eller kan vara part i ett sådant konfidentiellt samarbete, kan de identifikationer, vilkas betydelse är störst när det gäller att skydda den nationella säkerheten, inte överlåtas till HAVARO-systemet.

Syftet med de dataskyddsåtgärder som 272 § i informationssamhällsbalken möjliggör, inklusive HAVARO-systemet, är att genomföra dataskyddet genom att skydda enskilda målorganisationer mot intrång som riktar sig mot dem. Avsikten med dataskyddsåtgärderna är inte att täcka de behov av information som hänför sig till avvärjandet av verksamhet som äventyrar den nationella säkerheten. För den som utför dataskyddsåtgärder är sådan information som är väsentlig med tanke på upprätthållandet av den nationella säkerheten, såsom skälen till, förhållandena, förövarna och bakgrundmotiven till allvarligare dataskyddsintrång, inte viktig.

5.3 Befogenheter för inhämtande av information

Polisens och försvarsmaktens behörighet att använda hemliga metoder för att inhämta information har i lagstiftningen bundits till begreppet brott. Med förhindrande av brott avses i polislagen åtgärder som syftar till att förhindra brott, försök till brott och förberedelse till brott, när det utifrån iakttagelser av en persons verksamhet finns grundad anledning att anta att personen i fråga kommer att göra sig skyldig till brott, samt åtgärder som syftar till att avbryta ett redan påbörjat brott eller begränsa den direkta skada eller fara som brottet medför. Hemliga metoder för inhämtande av information får användas för förhindrande av förberedelse även i det fallet att förberedelsen av brottet i fråga inte har kriminaliserats.

Även om de hemliga metoderna för inhämtande av information får användas också för att förhindra förberedelsen av brott, och metodernas användningsområde därmed är omfattande, är det klart att hemliga metoder för inhämtande av information i dagens läge inte kan användas enbart för att inhämta underrättelseinformation om sådan verksamhet som t.ex. hotar den nationella säkerheten som inte har framskridit till stadiet för förberedelse av brott eller om vilket inte har föreskrivits att det är straffbart.

5.4 Iakttagelser gällande den internationella jämförelsen

I alla de jämförbara länder som granskas i betänkandet finns lagstiftning om underrättelse. I lagstiftningen om underrättelse kan ingå bestämmelser om inhämtande av information via datanätsomgivningen. Hur exakt regleringen är, varierar från land till land. Av detta skäl kan man inte av lagstiftningen i jämförelseländerna dra några direkta slutsatser om de enskilda metoder för inhämtande av information som är i användning. Det förekommer också skillnader i hur exakt de hot har specificerats på lagnivå för vilkas avvärjning information får inhämtas.

I jämförelseländerna ligger ansvaret för underrättelseverksamheten antingen på en underrättelsemyndighet eller alternativt har behörigheten delats mellan civila och militära underrättelsetjänster. Uppdelningen av underrättelsebefogenheterna mellan civila och militära myndigheter baserar sig i regel på om det är fråga om ett hot av civil eller militär art. Verksamheten vid underrättelsetjänsterna leds och styrs i allmänhet av försvarsministeriet och/eller inrikesministeriet. Uppdragen gällande inhämtande av information kan komma från statsledningen, de styrande ministerierna eller t.ex. försvarsmaktens ledning.

I jämförelseländerna har det ansetts viktigt att lagstifta om övervakningen av underrättelseverksamheten. Former för övervakningen är vid sidan av förvaltningsområdets interna övervakning också både parlamentarisk och utomstående juridisk övervakning. Den juridiska övervakningen utförs av en part som är oberoende av underrättelsetjänsten. Det kan t.ex. vara fråga om en permanent självständig övervakningskommitté eller granskningsnämnd. Övervakningsorganet har i typiska fall till uppgift att antingen på eget initiativ eller till följd av klagomål övervaka verksamhetens laglighet samt de metoder som används vid inhämtandet av information. De organ som utför övervakningen har i typiska fall obegränsat tillträde till underrättelsetjänstens lokaler och dokument. Övervakningsorganets medlemmar har tystnadsplikt. Övervakningsorganen rapporterar i allmänhet om sina upptäckter både i enskilda fall och i sina årsrapporter till den minister som styr underrättelseverksamheten och till den som är föremål för övervakningen. Målet med den juridiska övervakningen är också att trygga individens rättsskydd i enlighet med europeiska konventionen om mänskliga rättigheter.

Vidare ingår i jämförelseländernas lagstiftning bestämmelser t.ex. om att de underrättelsemetoder som begränsar integritetsskyddet kommer i fråga först i sista hand, om de tillståndsförfaranden som hänför sig till användningen av dessa metoder samt om behandlingen av de personuppgifter som inhämtats.

5.5 Relationen mellan säkerhetsmyndigheternas uppgifter och befogenheter

I kapitel 3.1 i betänkandet behandlas Skyddspolisens och försvarsmaktens uppgifter. Ett gemensamt drag för dessa uppgifter är att de gäller avvärjning av hot som riktar sig mot den nationella säkerheten. Avvärjningen av hot förutsätter att de kan upptäckas och att information om dem fås tillräckligt tidigt.

Vid sidan av att förebygga och avslöja brott och i mindre mån utreda sådana har Skyddspolisen till uppgift att avvärja sådana förehavanden som kan äventyra stats- och samhällsordningen eller rikets inre eller yttre säkerhet. Begreppet förehavande preciseras inte desto mera i polisförvaltningslagen eller förarbetet till den. Vid förehavanden kan det inte anses vara fråga om brott, vilket gör att det i ämbetsverkets uppgift till denna del är fråga om ett underrättelseuppdrag och inte ett uppdrag som syftar

till att avvärja ett brott. Det finns inga bestämmelser om befogenheter gällande underrättelse.

Vid försvarsmakten svarar den militära kontraunderrättelsen för brottsbekämpningen - förhindrandet och avslöjandet av brott. Separat från den militära kontraunderrättelsen finns militärunderrättelsen, där en allmän uppgift är att bevaka utvecklingen i Finlands säkerhetspolitiska omgivning, fastställa förändringarna i omgivningen och producera information om det rådande läget för att en militärstrategisk lägesbild ska kunna utformas. Ett särskilt mål för militärunderrättelsens inhämtande av information är den militärpolitiska och militära utvecklingen i närområdet. Militärunderrättelsens uppgifter är inte att avvärja brott. Det finns ingen lagstiftning om militärunderrättelse.
Det finns inte heller några bestämmelser om underrättelsebefogenheten för de myndigheter som avvärjer hot som riktar sig mot den nationella säkerheten och inte heller om fördelningen av dessa befogenheter mellan civila och militära myndigheter. I den nuvarande lagstiftningen grundar sig myndigheternas befogenheter att inhämta information enbart på brottsbekämpning och inte på underrättelse.

De osäkerhetsfaktorer som anknyter till den föränderliga säkerhetspolitiska omgivningen framhäver behovet att producera objektiv, certifierad och analyserad information om de säkerhetshot som riktar sig mot landet både för det politiska beslutsfattandet och som stöd för säkerhetsmyndigheternas beslutsfattande. Endast sanningsenlig information som erhålls på ett så tidigt stadium som möjligt om vilka avsikter och planer de parter har som ligger bakom hoten garanterar tillräcklig förmåga att varna om dessa på förhand. Tillgången på information på ett tidigt stadium förbättrar det finska samhällets möjligheter att förbereda sig på hot och bredda det metodutbud med hjälp av vilket det kan förhindras att hoten blir verklighet. Också med tanke på beredskapen inför undantagsförhållanden är det nödvändigt att information om de militära hot som riktas mot landet kan inhämtas redan under normala förhållanden.

Nuläget kan anses otillfredsställande med beaktande av de förändringar som har skett i den säkerhetspolitiska omgivningen. Det bör säkerställas att det finska samhället kan fungera också om särskilt allvarliga yttre hot samt dåd som riktar sig mot den kritiska infrastrukturen uppkommer. Med tanke på den nationella säkerheten är det viktigt att på ett tillräckligt tidigt stadium få information om de förändringar som sker i den finska säkerhetspolitiska omgivningen, inte endast sådant inhämtande av information som strävar efter att genomföra en förundersökning. Centralt vore att inhämta information om det rådande läget och analysera dess betydelse med tanke på landets nationella säkerhet.

6 UTVECKLINGSFÖRSLAG

Finlands yttre säkerhetspolitiska omgivning och krigföringens karaktär förändras med accelererande fart. Därför bör myndigheternas metoder för inhämtande av information utvecklas. Med nuvarande befogenheter att agera kan man inte tillräckligt effektivt och på ett tillräckligt tidigt stadium upptäcka hot och inte heller vidta de åtgärder som dessa skulle förutsätta, inklusive att ge en militär förvarning. Spridningen och användningen av felaktig information framhäver säkerhetsmyndigheternas behov att producera objektiv, säkerställd och analyserad information som stöd för den högsta statsledningens och militärt beslutsfattande.

Underrättelse är en omfattande helhet i vilken ingår flera olika underrättelse- och spaningsmetoder. Såsom det framgår av den internationella jämförelsen, stiftar staterna i typiska fall inte lagar bara om en underrättelsemetod. Ingen enskild underrättelsemetod ger nödvändigtvis all den information som behövs gällande den nationella säkerheten, utan informationen blir man tvungen att inhämta och säkerställa med flera underrättelsemetoder som stöder varandra.
Nedan beskrivs tre sådana underrättelsemetoder som enligt arbetsgruppens bedömning skulle ge särskilt betydelsefull information med tanke på den finska nationella säkerheten. Dessa är datatrafikspaning, personbaserad inhämtning utomlands samt spaning i utländska datasystem. Underrättelsemetoderna ersätter inte varandra, eftersom de till sin art delvis är olika. Med datatrafikspaning är syftet framför allt att upptäcka internationella hot. Med personbaserad inhämtning utomlands och spaning i utländska datasystem inhämtas huvudsakligen information om hot som redan har identifierats.

6.1 Datatrafikspaning

6.1.1 Allmänt

Den underrättelse som riktas mot kommunikationen har på grund av de ändringar som behandlas i kapitel 2 i betänkandet en central roll när det gäller att upptäcka hot som riktar sig mot den nationella säkerheten. Största delen av den globala kommunikationen mellan enskilda personer, företag och offentliga aktörer förmedlas i dagens läge i ett fast datakommunikationsnät. De datakommunikationsanordningar och datakommunikationstrådar som finns på finskt område förmedlar utöver landets interna meddelandekommunikation också internationell meddelandekommunikation. Internationell meddelandekommunikation innehåller gränsöverskridande kommunikation som sänds från Finland och som kommer till Finland samt internationell transiteringskommunikation, där både begynnelse- och slutpunkten finns utanför Finland. Till följd av att kommunikationstekniken utvecklas är den information som förmedlas i datakommunikationstrådarna central för att man ska kunna upptäcka hot.

Betydelsen av den trådförmedlade datakommunikationen med tanke på att de hot som riktas mot den nationella säkerheten ska kunna avvärjas har erkänts i flera av de västländer som kan jämföras med Finland. Av den internationella jämförelsen framgår att lagstiftningen i de flesta jämförelseländerna gör det möjligt för myndigheterna att inrikta spaning på kabelnät eller också planeras dylik lagstiftning.

I datatrafikspaning är det frågan om att myndigheten inhämtar information som är väsentlig för den internationella säkerheten ur datatrafiken och dess innehåll. Datatrafikspaning kan generellt inriktas på statens interna eller gränsöverskridande datatrafik. För att verksamheten ska kunna realiseras förutsätts att den myndighet som utför spaningen har tillträde till datatrafiktrådarnas anslutningspunkter. I typiska fall inriktas inhämtandet av information via spaning med hjälp av automatiserade sökbegrepp som gallrar i datatrafiken. Då begränsas skyddet för ett konfidentiellt meddelande vid spaningen i datatrafiken. När utvecklingsförslagen övervägs måste kraven i de internationella fördrag som binder Finland och grundlagen beaktas.

6.1.2 Kraven i de internationella fördragen om mänskliga rättigheter och i grundlagen

6.1.2.1 Förenta nationernas konvention om medborgarrättigheter och politiska rättigheter

Den internationella konvention om medborgarrättigheter och politiska beslut, som FN:s generalförsamling godkände år 1966, (den s.k. MP-konventionen; FördrS 8/1976) blev bindande för Finland år 1976.

Med tanke på skyddandet av konfidentiell kommunikation är konventionens artikel 17 central. Enligt den får ingens privatliv, familj, hem eller brevväxling godtyckligt eller olagligt kränkas och inte heller får attacker som sårar hans eller hennes heder eller rykte utföras. Dessutom har var och en rätt till skydd av lagen mot sådana kränkningar eller attacker. Från skyddet enligt artikeln får avvikelse göras endast under ett allmänt nödläge, som hotar den nationella existensen och som officiellt har deklarerats som ett sådant nödläge.
Det förbud mot att ingripa i privatliv och brevväxling som fastslås i artikel 17 i MP-konventionen är inte absolut, utan förbudet gäller ”godtyckligt” och ”olagligt” ingripande i rättigheterna. Konventionsstaterna kan i sin nationella lagstiftning föreskriva om sådana situationer som berättigar till ett ingripande och om de metoder som ska användas vid ingripandet. Alla konventionsstater har följaktligen föreskrivit om ingripande i rättigheter som görs i syfte att bekämpa brott och många också om ingripande i rättigheter som görs i syfte att upprätthålla den nationella säkerheten.

Verkställandet av MP-konventionen övervakas av FN:s människorättskommitté, som kontinuerligt utvecklar tolkningen av bestämmelserna i konventionen. I människorättskommitténs allmänna kommentar nr 16 från år 1988 (A/43/20) tolkas innehållet i artikel 17 bl.a. med tanke på elektronisk kommunikation. Enligt kommentaren är det

inte tillräckligt att det i lag har föreskrivits om ingripande i skyddet för privatlivet. Den lagstiftning som berättigar till ingripande får inte vara godtycklig till sitt innehåll och tillämpningen av den får inte heller vara godtycklig. Lagstiftningen måste stå i överensstämmelse med bestämmelserna i och målen med MP-konventionen, och i den ska de förhållanden där det är tillåtet att ingripa specificeras noggrant. Ett beslut om en åtgärd som ingriper i integritetsskyddet ska kunna fattas endast för ett specifikt fall och på åtgärd av en myndighet som fastslås i lag och den information som samlas med hjälp av ingripandet ska vara nödvändig med tanke på samhällets intressen (”essential in the interests of society”). Information som anknyter till en persons privatliv får inte användas i syften som står i strid med MP-konventionen.

Flera besvär om intrång i artikel 17 som gäller integritetsskydd har anförts med stöd av MP-konventionens tillvalsprotokoll, men kommittén har hittills inte behandlat frågor med anknytning till datanätssäkerheten och elektronisk kommunikation. Det kan anses sannolikt att frågor med anknytning till den elektroniska kommunikationens konfidentialitet kommer att bli mera synliga i människorättskommitténs arbete[34].

6.1.2.2 Artikel 8 i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna

När man bedömer om det ska tillåtas att en lag stiftas om datakommunikationsunderrättelse är europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, som ingicks inom Europarådet år 1950, och till vilken Finland anslöt sig år 1989 (EMK; FördrS 63/1999) av större praktisk betydelse än MP-konventionen. Att människorättskonventionen följs övervakas av Europeiska människorättsdomstolen (EMD), som i detta syfte behandlar och avgör besvär som gäller förbrytelser mot konventionen. EMD har i många avgöranden tagit ställning till hur rätten till skydd för konfidentiellt meddelande enligt människorättskonventionen bör tolkas. Flera av dessa avgöranden gäller elektronisk kommunikation och några datakommunikationsunderrättelse eller därmed jämförbara former av myndighetsverksamhet.

Enligt artikel 8(1) i europeiska människorättskonventionen har var och en rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Enligt artikel 8(2) i EMK 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 den nationella eller allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.

[34] Till exempel Förenta staternas fjärde periodiska rapport om verkställandet av MP-konventionen (CCPR/C/USA/4) behandlar i detalj övervakningen av elektronisk datakommunikation. I sina tilläggsfrågor till Förenta staterna begär kommittén ytterligare upplysningar gällande den juridiska övervakningen av National Security Agencys elektroniska informationsförmedling såväl inom statens territorium som också utanför det (CCPR/C/USA/Q/4).

Enligt etablerad avgörandepraxis i europeiska människorättsdomstolen inbegriper begreppen privatliv och korrespondens, som nämns i artikel EMK 8(1), både telefonkommunikation, e-postkommunikation och annan elektronisk kommunikation som ska anses konfidentiell *(bl.a. Klass och andra mot Tyskland, Kopp mot Schweiz, Copland mot Förenade konungadömet, Liberty och andra mot Förenade konungadömet)*. Skyddet omfattar både kommunikationens innehåll och kommunikationens identifikationsuppgifter *(bl.a. Malone mot Förenade konungadömet, Weber och Saravia mot Tyskland, P.G. och J.H. mot Förenade konungadömet)*. I fråga om identifikationsuppgifterna har domstolen särskilt konstaterat att uppgifter t.ex. om de telefonnummer som en person har kommunicerat till utgör en organisk del av kommunikationen. Överlämnandet av sådana uppgifter till en myndighet utan samtycke av personen i fråga utgör också det ett ingripande i dennes privatliv *(Malone mot Förenade konungadömet)*.

Myndigheten behöver inte de facto behandla uppgifterna för att det ska vara fråga om ingripande i privatliv, utan som ingripande ska anses det att myndigheten samlar in och sparar dem för senare användning *(Marper mot Förenade konungadömet)*. Enbart det att sådan lagstiftning existerar, som gör det möjligt att hemligt observera kommunikationsförbindelser, ingriper i de rättigheter som artikel 8 i EMK garanterar kommunikationens parter och även potentiella parter *(Klass mot Tyskland, Liberty och andra mot Förenade konungadömet)*. Övervakningens potentiella objekt måste då ha rätt till ett effektivt rättsmedel som artikel 13 i EMK garanterar inför den nationella myndigheten. Enligt artikel 13 EMK ska var och en, vars i konventionen angivna fri- och rättigheter kränkts, ha tillgång till ett effektivt rättsmedel inför en nationell myndighet även i det fall att kränkningen utförts av någon i offentlig ställning.

Även om sannolikheten för hemlig övervakning av en person är liten, måste han eller hon i EMD kunna låta undersöka sitt påstående om att rättigheterna enligt artikel 8 i EMK har blivit kränkta, om effektiva nationella rättsmedel saknas *(Kennedy mot Förenade konungadömet)*.

Tillåtet ingripande i rättigheter enligt artikel 8(1) EMK

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

Kravet på att ingripandet ska grunda sig på lag

Ingripande i de rättigheter som artikel 8 i EMK garanterar 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 myndighetens prövningsbefogenhet och sätten att använda prövningsbefogenheten ska tillräckligt klart fastställas i lag för att möjligheten till godtycklighet som ingår i hemligt användande av verkställighetsbefogenheten ska kunna avvärjas *(Malone mot Förenade konungadömet, Amann mot Schweiz, Telegraaf Media Nederland Landelijke Media B.V. och andra mot Nederländerna, Rotaru v. Rumänien).*

EMD har i sina avgöranden upprepade gånger betonat att en lag som möjliggör att hemliga myndighetsåtgärder ingriper i skyddet för privatliv ska vara förenlig med rättsstatsprinciperna, tillgänglig för medborgarna samt till sin art sådan att medborgarna kan förutse vilka följder tillämpningen av den har på dem själva *(bl.a. Kruslin mot Frankrike, Huvig mot Frankrike, Lambert mot Frankrike)*. Lagen får inte vara sådan att den möjliggör att hemlig observation riktas slumpmässigt mot vem som helst *(Amann mot Schweiz).*

När det bedöms om kravet på förutsebarhet uppfylls, ska det beaktas att folkrepresentationen också utfärdar förordningar och myndighetsföreskrifter vid sidan av egentliga lagar. Bestämmelserna i en lag, som kan vara mycket generella, kan preciseras med instrument på en lägre nivå. Dessa ska dock offentliggöras – sådana interna myndighetsföreskrifter som inte är tillgängliga för medborgarna uppfyller inte kravet på förutsebarhet *(t.ex. Silver och andra mot Förenade konungadömet, Malone mot Förenade konungadömet)*. En allmänt tillgänglig lag ska definiera åtminstone kvaliteten på och omfattningen av de observationsfullmakter som ska användas hemligen, de personkategorier som fullmakterna får användas mot, arten av den verksamhet som ger anledning till att använda fullmakterna, de förfaranden som ska följas när den information som inhämtas med hjälp av fullmakterna undersöks, utnyttjas, sparas, distribueras vidare och undanröjs, bestämmelser om övervakningen av fullmakterna och om rättsmedel som gäller dem *(Amann mot Schweiz, Valenzuela Conreras mot Spanien, Prado Bugallo mot Spanien, Shimovolos mot Ryssland)*. De krav som ska ställas på att lagstiftningen är förutsebar gäller oberoende av om det är fråga om observation grundad på ett brott, vilken gäller enskilda personers meddelandekontakter, eller allmän övervakning i stor skala av meddelandekontakter som grundar sig på hot *(Weber och Saravia mot Tyskland, Liberty och andra mot Förenade konungadömet).*

EMD har bedömt hur väl den allmänna övervakningen i stor skala av internationella meddelandekontakter stämmer överens med människorättskonventionen i två viktiga avgöranden. I fallet *Liberty och andra mot Förenade konungadömet* ansåg domstolen att den nationella lagstiftning som möjliggjorde allmän övervakning till sin art var sådan att den inte uppfyllde kravet i artikel 8(2) i EMK om att hemlig observation ska

grunda sig på lag. I fallet *Weber och Saravia mot Tyskland* kom domstolen till motsatt resultat – den nationella lagstiftningen uppfyllde de krav som ställts på lagens kvalitet och var därmed förenlig med människorättskonventionen.

I fallet *Liberty och andra mot Förenade konungadömet* var det frågan om en storskalig övervakning av telefontrafiken till utlandet, som signalspaningsverket, som lyder under försvarsministeriet i Storbritannien, hade utfört. Inom ramen för denna övervakning kunde man samtidigt avlyssna t.o.m. 10 000 telefonlinjer. I sig var frågan obestridlig, eftersom verksamheten grundade sig på en nationell lag.[35] Enligt denna lag kunde inrikesministern ge olika säkerhetsmyndigheter tillstånd (”warrant”) att inrikta inhämtande av information på meddelandekontakter mellan Storbritannien och utlandet. I tillstånden definierades de meddelandekontakter som inhämtandet av information kunde riktas mot på en mycket allmän nivå (t.ex. ”alla meddelanden som förmedlas i sjökablar mellan Storbritannien och det övriga Europa”). I samband med att tillstånd beviljades skulle inrikesministern definiera vilket material inhämtandet av information skulle gälla. Enligt lagen räckte det emellertid som definition att den information som skulle inhämtas enligt inrikesministerns uppfattning behövdes antingen för att upprätthålla den nationella säkerheten, förebygga eller avslöja allvarlig brottslighet eller för att trygga landets ekonomiska intressen. När tillstånd beviljades skulle inrikesministern också meddela sådana hemliga föreskrifter som han eller hon ansåg nödvändiga för att säkerställa att sådana meddelanden som inte omfattades av tillståndet inte skulle bli granskade och att de meddelanden som skulle granskas avslöjades eller kopierades endast i behövlig omfattning. I lagen fanns inga närmare bestämmelser om dessa föreskrifters innehåll eller område. Efter att ha fått tillstånd av inrikesministern formade säkerhetsmyndigheterna självständigt de automatiska sökbegrepp med hjälp av vilka den information som gällde den nationella säkerheten eller andra i lagen nämnda intressen filtrerades ur totalmassan av kommunikation. Säkerhetsmyndigheterna hade sina egna interna bestämmelser om på vilka grunder de uppgifter som erhölls som resultat av filtreringen behandlades, sparades, delades och undanröjdes, men dessa bestämmelser var inte offentliga eller allmänt tillgängliga.

I sitt avgörande i saken konstaterade EMD att enligt lagen kunde inrikesministerns tillståndsbeslut omfatta vilket meddelande som helst, vilket gjorde att vilket som helst meddelande som vem som helst skickade till utlandet eller fick därifrån kunde fångas upp. Följaktligen hade den verkställande makten i fråga om att infånga utländska meddelanden beviljats en i praktiken obegränsad prövningsbefogenhet. Lagen medgav också en omfattande prövningsmarginal i fråga om det vilka meddelanden som de facto granskades. I detta hänseende var det tillräckligt att inrikesministern ansåg granskningen nödvändig med tanke på den nationella säkerheten eller andra i lagen nämnda och allmänt formulerade intressen. I lagen fanns inga närmare bestämmelser om behandlingen av meddelanden som inte omfattades av tillståndet och de bestämmelser som inrikesministern gett i saken var inte offentliga. I sammandrag konstate-

[35] Interception of Communications Act 1985

rade EMD att gränserna för den mycket vida prövningsbefogenheten som beviljats för infångandet och granskandet av meddelanden inte genom den nationella lagen hade anvisats tillräckligt klart för den verkställande makten. I synnerhet hade det inte påvisats offentligt hur gallringen, användningen, förvaringen och förstöringen av infångat material skulle genomföras. Således svarade Storbritanniens signalspaningslagstiftning inte mot de kvalitetskrav som ställdes i artikel 8(2) i EMK och ett brott mot människorättskonventionen hade begåtts.

I fallet *Weber och Saravia mot Tyskland* var det frågan om storskalig s.k. strategisk övervakning som Tysklands underrättelsetjänst BND hade bedrivit i fråga om mobiltelefontrafiken mellan Tyskland och utlandet. Om sådan övervakning föreskrivs i nationell lag.[36] Enligt denna lag fick strategisk övervakning av mobiltelefontrafiken bedrivas för att avvärja vissa särskilt nämnda hot som riktade sig mot den nationella säkerheten. Sådana i lagen definierade hot var en militär attack på Tyskland, terrordåd som skulle genomföras i Tyskland och till sin art var internationella, internationell smuggling av vapen, storskalig import av droger, penningförfalskning utomlands och penningtvätt med anknytning till ovan nämnda fenomen. Tillstånd till varje enskild strategisk övervakningsuppgift beviljade förbundsstatens minister efter att först ha hört det parlamentariska övervakningsorganet med anledning av tillståndsansökan. De automatiska sökbegrepp med hjälp av vilka avsikten var att filtrera mobiltelefontrafiken skulle framgå både av BND:s tillståndsansökan och av det tillstånd som ministern beviljade. Lagen innehöll bestämmelser om hur det material som hade filtrerats skulle behandlas och i vilka fall uppgifter om personer, som dykt upp genom filtreringen, fick användas för att förebygga, avslöja och reda ut brott. Likaså innehöll lagen bestämmelser om när den filtrerade informationen skulle räknas som inte hörande till saken och hur man skulle förfara med sådan information. Vidare föreskrevs det i lagen om giltighetstiderna för övervakningstillstånden, om hur länge filtrerade uppgifter skulle sparas, om förstörande av uppgifter samt om de grunder och förutsättningar under vilka uppgifterna kunde lämnas över till andra myndigheter.

EMD ansåg att den tyska lagstiftningen uppfyllde de krav på kvalitet och förutsebarhet som ställdes för lagen med stöd av artikel 8(2) i EMK. Viktigt i detta hänseende var bl.a. det att lagen definierade de hot för vilkas avvärjande övervakning kunde bedrivas. Lagen ansågs också erbjuda en tillräcklig anvisning om vilka personkategorier övervakningen enligt lagen kunde riktas mot.[37] De automatiska sökbegrepp som ska användas för att inrikta övervakningen ska direkt med stöd av lagen framgå av de tillstånd som beviljas för övervakningen, varvid den myndighet som bedriver övervakning inte har obegränsad prövningsrätt när det gällde att definiera dem. Med tanke på att kravet på förutsebarhet skulle uppfyllas var det också av betydelse att lagen defini-

[36] Gesetz für Beschrenkung des Brief-, Post- und Fernmeldegeheimnisses 1968 och Verbrechenbekämpfungsgesetz 1994.

[37] ”Personer som deltar i internationella mobiltelefondiskussioner som förmedlas via satellit och vilkas diskussionsinnehåll är sådant att det filtreras för fortsatt granskning utgående från ett automatiskt sökbegrepp som anknyter till en militär attack som riktas mot Tyskland, internationell terrorism o.a. dylikt”.

erade maximitider för tillståndens giltighet och innehöll bestämmelser om de förfaranden som skulle följas när uppgifterna granskades och utnyttjades. Likaså var det enligt EMD av betydelse att lagen föreskrev om de begränsningar och villkor som skulle följas vid vidareöverlåtelse av uppgifter samt om de förhållanden där uppgifterna skulle förstöras. I sitt avgörande i fallet *Weber och Saravia* konstaterade EMD även särskilt att den allmänna övervakningen av meddelandekontakter som bedrivs på tysk mark i princip kan kränka andra länders statssuveränitet fastän den andra parten i meddelandekontakterna skulle befinna sig i ett sådant annat land.

Den nationella säkerheten som ett intresse som berättigar till ingripande

Den nationella säkerheten är ett av de intressen som enligt artikel 8(2) i EMK kan berättiga till att ingripa i skyddet för privatlivet. EMD har i sin rättspraxis endast sällan ifrågasatt de svarande staternas påståenden att ingripandet har skett med hänsyn till den nationella säkerheten.[38] 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 artikel 8 i EMK garanterar. Bakom detta ligger att den nationella säkerheten av tradition omfattas av staternas suveränitet *(Bucur och Toma mot Rumänien)*. Utgående från domstolens avgörandepraxis är det klart att åtminstone det militära försvaret, terrorismbekämpningen och bekämpningen av olovlig underrättelseverksamhet omfattas av den nationella säkerheten *(bl.a. Klass mot Tyskland, Weber och Saravia mot Tyskland).* Emellertid kan hot av flera slag riktas mot den nationella säkerheten och det är svårt att förutse eller på förhand definiera dem. Av detta följer att ett klargörande av begreppet i första hand måste lämnas till nationell praxis *(Kennedy mot Förenade konungadömet)*. Staternas prövningsrätt kan för sin del ökas av det att den nationella säkerhetens gräns mot andra tillåtna grunder (bl.a. allmän säkerhet och förhindrande av oordning eller brottslighet) att ingripa i de rättigheter som artikel 8(1) i EMK garanterar kan uppfattas som svävande från fall till fall.[39]

Nödvändigheten av ingripande i ett demokratiskt samhälle

Det tredje och sista villkoret för att myndigheterna ska få ingripa i användningen av de rättigheter som artikel 8 i EMK garanterar är att ingripandet är nödvändigt i ett demokratiskt samhälle. Ordet ”nödvändigt” som används i den svenska versionen av artikeln måste i någon mån anses oförmöget till särskiljande, emedan EMD har uttryckt följande om betydelseinnehållet i den engelska motsvarigheten: *” the adjective ”necessary” is not synonymous with ”indispensable”, neither has it the flexibility of such expressions as ”admissible”, ”ordinary”, ”useful”, ”reasonable” or ”desirable”*

[38] EMD har visserligen förhållit sig tvivlande till exempel till det, om uppgifter om en persons politiska inriktning, vilka gällde år 1937, kan ha betydelse för den nationella säkerheten sextio år senare (Rotaru mot Rumänien). Domstolen har också till exempel ansett att smuggling av cigaretter i alla fall inte kan höra till den nationella säkerhetens område även om en militärflygplats hade utnyttjas vid smugglingen (Dumitru Popescu mot Rumänien).
[39] TIll en dylik partiell överlappning av intressen hänvisas t.ex. i avgörandet Silver och andra mot Förenade konungadömet

(Handyside mot Förenade konungadömet). Man torde alltså behöva anse att den nödvändighet som artikeln avser, placerar sig någonstans mellan oersättlig och behövlig. Förutsättningen ’nödvändigt i ett demokratiskt samhälle’ innehåller det att ingripandet i rättigheter bör svara mot ett tvingande samhälleligt behov *(correspond to a pressing social need).* Av förutsättningen följer också att ingripandet ska vara förenligt med proportionalitetsprincipen: ingripandet ska stå i ett förnuftigt förhållande till det mål som artikel 8(2) i EMK tillåter, vilket åberopas som berättigande grund *(bl.a. Gillow mot Förenade konungadömet, Silver och andra mot Förenade konungadömet, Handyside mot Förenade konungadömet).*

Bedömandet av om ett ingripande är nödvändigt, såväl med tanke på ett samhälleligt behovs tvingande natur som också med tanke på proportionaliteten, ankommer först och främst eller åtminstone i en första fas på den nationella lagstiftaren och de nationella myndigheterna *(Silver och andra mot Förenade konungadömet, Handyside mot Förenade konungadömet).* När en sådan bedömning görs har de nationella parterna ett visst utrymme för sin prövning, vars omfattning fastställs bl.a. av det vilken av rättigheterna enligt EMK ingripandet gäller, hur djupgående ingripande det är frågan om samt vilket av de i artikel 8(2) i EMK tillåtna målen som är den grund som ger rätt att ingripa. Utrymmet för prövningen är vidare än normalt när berättigande grund är den nationella säkerheten *(Klass och andra mot Tyskland, Leander mot Sverige)*. I frågor som gäller den nationella säkerheten gäller statens ganska vida prövningsrätt också de konkreta medel och metoder med hjälp av vilka den skyddar intresset i fråga. I sitt avgörande Weber och Saravia mot Tyskland ansåg EMD att staten inom ramen för den prövningsrätt som ankom på den kunde föreskriva om en storskalig övervakning av kommunikationskontakter som en metod för att skydda sin nationella säkerhet. Det var fråga om ett nödvändigt ingripande i ett demokratiskt samhälle i rättigheter som artikel 8 i EMK garanterar för privata rättssubjekt.

Å andra sidan har EMD betonat att myndigheternas hemliga observations- och övervakningsfullmakter, som används i den nationella säkerhetens namn, kan utgöra en fara för den demokratiska samhällsordningen *(bl.a. Antunes Rocha mot Portugal)*. Av detta skäl bör staten ordna en oberoende övervakning av hur de används och effektiva rättsmedel. Avgöranden från de instanser som utför laglighetsövervakning bör ha en juridiskt bindande verkan i relation till de övervakade parterna – med tanke på skyddandet av demokratin är det inte tillräckligt att laglighetsövervakarna kan styra de parter de övervakar med hjälp av rekommendationer *(Segerstedt-Wiberg och andra mot Sverige)*. Den juridiska reglering som gäller hemliga fullmakter bör vara offentlig och så exakt att laglighetsövervakning kan utövas på ett trovärdigt sätt *(Liberty och andra mot Förenade konungadömet)* dock utan att syftet med hemligt inhämtande av information äventyras *(Segerstedt-Wiberg och andra mot Sverige)*. Med tanke på skyddandet av demokratin är det också av betydelse att folkrepresentationen för sin del är med och övervakar de hemliga observationsfullmakterna *(Campbell mot Förenade konungadömet, Leander mot Sverige).*

6.1.2.3 Europeiska unionens stadga om de grundläggande rättigheterna

Europeiska unionens stadga om de grundläggande rättigheterna, som trädde i kraft år 2009, definierar de grundläggande rättigheter som gäller på unionens nivå. Medlemsstaterna är skyldiga att följa stadgan om de grundläggande rättigheterna alltid när de tillämpar unionens rätt. Enligt artikel 7 i grundrättsstadgan 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. Uppgifterna 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 fastslår de genom stadgan garanterade rättigheternas räckvidd. Enligt stycke 1 i artikeln ska varje begränsning i utövningen 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 stycke 3 i samma artikel sägs 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. Detta 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 EMK. I ingressen till stadgan konstateras särskilt att de rättigheter som ska bekräftas har sin grund förutom i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna också i rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna. EMD:s omfattande avgörandepraxis som gäller artikel 8 i människorättskonventionen ska således anses vara relevant också för tolkningen av artikel 7 i stadgan.

Trots det som sägs ovan ankommer övervakningen av respekten för de mänskliga rättigheterna i enlighet med stadgan inte på EMD utan på Europeiska unionens domstol (EUD) och på de nationella domstolarna. Med tanke på datatrafikspaningen är den dom som EUD gav i april 2014 av betydelse[40], genom vilken domstolen förklarade att direktivet Data Retention från år 2006 var ogiltigt. Direktivet hade gett unionens medlemsstater en skyldighet att föreskriva om ett omfattande förvarande av teleidentifikationsuppgifter för de behov som bekämpningen och undersökningen av allvarliga brott hade.

[40] Dom i de förenade målen C-293/12 och C-594/12.

EUD ansåg i sin ovan nämnda dom att direktivet Data Retention stred mot den proportionalitetsprincip som avses i artikel 52.1 i grundrättsstadgan. Proportionalitetsprincipen inbegriper att en begränsning av en grundläggande rätt är nödvändig. När EUD bedömde hur nödvändig den begränsning av rättigheterna var, som hade gjorts genom direktivet Data Retention, uppmärksammade domstolen att skyldigheten att förvara teleidentifikationsuppgifter, om vilken direktivet föreskrev, gällde alla personer, alla sätt att kommunicera elektroniskt och nästan alla identifikationsuppgifter utan någon som helst urskillnad, begränsning eller något undantag som skulle ha baserat sig på målet att förhindra allvarlig brottslighet. Förvaringsskyldigheten omfattade också alla sådana personers teleidentifikationsuppgifter i fråga om vilka det inte fanns något som helst bevis ens för avlägsen eller indirekt koppling till brottslighet. Således måste det anses att direktivet i praktiken ingrep i rättigheterna för varje person som vistades inom EU:s territorium.

Enligt EUD borde direktivet ha innehållit åtminstone en del[41]av följande element för att det skulle vara förenligt med proportionalitetsprincipen:

- Något slags objektiva gränser med anknytning till direktivets målsättning i fråga om det vilka personers teleidentifikationsuppgifter som får bevaras.
- En mera exakt definiering av de brott för vilkas avvärjande eller undersökning de nationella myndigheterna får bekanta sig med och använda de identifikationsuppgifter som ska bevaras. Till denna del hänvisar direktivet endast till ”allvarliga brott”, vilkas innehåll fastslås enligt varje medlemsstats nationella lagstiftning.
- Materiella och förfaringsmässiga förutsättningar för att bekanta sig med uppgifterna och använda dem. Som förutsättning för att bekanta sig med uppgifterna har det i direktivet inte ställts t.ex. tillstånd av domstol eller något annat oberoende organ, utan beslutet om förfarandet har lämnats fritt att bestämmas om i de nationella rättsakterna.
- Mera exakta bestämmelser om förvaringstiderna för identifikationsuppgifter. I direktivet föreskrivs att sex månader är den kortaste förvaringstiden utan att det görs någon skillnad i fråga om det, huruvida uppgifterna kan vara till nytta i brottsbekämpningen eller inte.
- För att garantera ett effektivt dataskydd tillräckliga garantier för att de uppgifter som ska bevaras inte missbrukas. Direktivet tillåter att teleföretagen beaktar ekonomiska aspekter när de definierar den skyddsnivå de tillämpar.
- Föreskrifter om att uppgifterna ska förvaras inom unionens territorium.

Riksdagens grundlagsutskott har i sitt utlåtande GrUU 18/2014 rd kommenterat EUD:s dom. Enligt utskottet ger domen inget direkt svar på hur den nationella lagstiftningen ska utformas för att uppfylla kraven på proportionalitet när det gäller pri-

[41] Enligt grundlagsutskottets ställningstagande grundar sig unionsdomstolens dom på en samlad bedömning av det aktuella direktivet (GrUU 18/2014 rd, s. 6)

vatlivet och personuppgifter. Man måste enligt utskottet dock utgå från att åtminstone sådana bestämmelser strider mot proportionalitetskravet som innebär omfattande, ospecificerad, långvarig och obegränsad förvaring av uppgifter i kombination med att myndigheter har ospecificerad och obegränsad tillgång till dessa uppgifter. Grundlagsutskottet konstaterade också att det utifrån domen förblir öppet huruvida det att skyldigheten att lagra uppgifter för myndigheternas behov i praktiken utsträcker sig till uppgifter om alla personer som använder elektroniska kommunikationsmedel i sig innebär en kränkning av proportionalitetskravet.[42]

I sin dom konstaterade EUD att i direktivet borde ha ställts objektiva gränser i anknytning till dess målsättning för det, vilka personers identifikationsuppgifter får förvaras. Dessutom borde direktivet närmare ha definierat de brott för vilkas bekämpning skyldigheten att förvara uppgifterna ställdes. Till denna del är det viktigt att vara medveten om att EUD:s dom inte egentligen skapar någon ny rätt. Den motsvarar europeiska människorättsdomstolens etablerade avgörandepraxis. Människorättsdomstolen har gett en större mängd avgöranden där den på motsvarande sätt som EUD:s dom men mera detaljerat har behandlat de element som en lag, som ingriper i skyddet för privatlivet, måste innehålla för att stämma överens med proportionalitetsprincipen och vara förutseende. Mera betydelsefulla i detta hänseende är människorättsdomstolens avgöranden som direkt gäller datatrafikspaning eller fenomen som står nära den, *Klass mot Tyskland (1978), Weber och Saravia mot Tyskland (2006) och Liberty och andra mot Förenade konungadömet (2008).*

6.1.2.4 Av Finlands grundlag föranledda krav på den lagstiftning som begränsar skyddet för konfidentiell kommunikation

Rättsstatsprincipen

Enligt 2 § 3 mom. i grundlagen ska det allmännas maktutövning grunda sig på lag och i all offentlig verksamhet ska lag noga följas. Om man genom underrättelselagstiftning skapar nya uppgifter för myndigheterna och befogenheter i anknytning till dem ska om både uppgifterna och befogenheterna föreskrivas i lag. Samtidigt ska de personer som är föremål för myndighetsbefogenheter garanteras rättsskydd genom en tillräcklig reglering.

De grundläggande rättigheterna

De grundläggande rättigheterna är i allmänhet inte ovillkorliga, även om bestämmelsen om grundläggande rättigheter har skrivits i en form som tryggar rättigheten och även om bestämmelsen inte innehåller ett lagstiftningsförbehåll eller någon annan hänvisning till lag. Härvid avgörs frågan om begränsning av en grundläggande rättighet i enlighet med de allmänna dogmer som gäller begränsning av grundläggande rättigheter.

[42] GrUU 18/2014 rd, s. 6

Grundlagsutskottet har härlett några allmänna krav gällande begränsning av de grundläggande rättigheterna ur systemet med grundläggande rättigheter som helhet och rättigheternas natur som rättigheter som är tryggade i grundlagen (GrUB 25/1994 rd s. 4–5). Sådana är kraven på

1. att de ska stiftas genom lag
2. lagen ska vara exakt och noga avgränsad
3. begränsningarna ska vara godtagbara
4. begränsningarna ska vara proportionella
5. kärnområdet i en grundläggande rättighet är okränkbart
6. rättsskyddsarrangemangen ska vara tillräckliga och
7. människorättsskyldigheterna ska följas.

Skyddet för hemligheten i fråga om ett förtroligt meddelande

Enligt 10 § i grundlagen är vars och ens privatliv, heder och hemfrid tryggade och brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbar. Bestämmelsens princip är att individen har rätt att leva sitt liv utan godtycklig eller oskälig inblandning från myndigheterna eller andra utomstående i hans eller hennes privatliv. Paragrafen tryggar var och en rätt till förtrolig kommunikation, utan att utomstående utan rätt får vetskap om innehållet i de förtroliga meddelanden som han eller hon sänder eller tar emot.[43]

Enligt 10 § 3 mom. i grundlagen kan genom lag bestämmas om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna ska kunna tryggas eller för att brott ska kunna utredas. Genom lag kan också bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång och säkerhetskontroll samt under frihetsberövande. Dessa möjligheter att begränsa skyddet för ett förtroligt meddelande har i samband med grundlagsreformen avsetts som en uttömmande förteckning (RP 309/1993 rd, s. 54). Till exempel med avvikelse från artikel 8 i europeiska människorättskonventionen nämner 10 § 3 mom. i grundlagen inte nationellt säkerhetsintresse som ett sådant intresse som skulle ge rätt att genom lag bestämma om begränsningar av hemligheten i fråga om ett förtroligt meddelande.

Grundlagsutskottet har ansett att det kan betraktas som utredning av brott enligt 10 § 3 mom. i grundlagen när åtgärder vidtas med anledning av en konkret och specificerad misstanke om brott trots att brottet ännu inte har omsatts i gärning.[44]

Grundlagens bestämmelse om hemligheten i fråga om ett förtroligt meddelande har formats så att den är instrument- och teknikneutral. Brev- och telefonhemligheten har

[43] RP 309/1993 rd
[44] GrUU 19/2008 rd, s. 3, GrUU 11/2005 rd, s. 3, GrUU 9/2004 rd, s. 3, GrUU 37/2002 rd, s. 3, GrUU 26/2001 rd, s. 3, GrUU 2/1996 rd

nämnts särskilt, men bestämmelsen tryggar generellt hemligheten i fråga om all slags förtrolig kommunikation.[45]

Grundlagsbestämmelsen om ett förtroligt meddelandes hemlighet har som första syfte att för utomstående skydda innehållet i ett meddelande som är avsett att vara förtroligt. Grundlagen tryggar vars och ens rätt att kommunicera förtroligt utan att utomstående orättmätigt får information om innehållet i förtroliga meddelanden som personen har sänt eller tagit emot. Detta innebär t.ex. skydd mot att brev eller andra slutna meddelanden öppnas eller förstörs samt mot att telefoner avlyssnas eller bandas. Bestämmelsen skyddar inte bara avsändaren utan det är frågan om en grundläggande rättighet för båda parterna i kommunikationen.[46]

Bestämmelsen skyddar inte innehållet i en diskussion som förs på hörbart avstånd och kan uppfattas med sinnet, men att avlyssna en diskussion som är avsedd att vara förtrolig genom att använda ett tekniskt hjälpmedel innebär begränsning i skyddet av ett förtroligt budskaps hemlighet.[47]

Genom grundlagsregleringen har man inte eftersträvat att ordna relationerna mellan kommunikationens parter eller deras beteende. Frågan om parterna i en förtrolig kommunikation har rätt att offentliggöra ett meddelande som var avsett att vara förtroligt måste avgöras på andra grunder.[48]

Ett förtroligt meddelandes identifikationsuppgifter

Utöver innehållet i meddelandet skyddar bestämmelserna i grundlagen också identifikationsuppgifterna i fråga om meddelandets avsändare och mottagare samt övriga uppgifter som kan ha betydelse för att meddelandet ska förbli förtroligt. Grundlagsutskottet har i sin praxis ansett att ett meddelandes identifieringsuppgifter faller utanför kärnområdet i den grundläggande fri- och rättigheten för sekretess i fråga om konfidentiella meddelanden[49]. I ett färskt utlåtande har utskottet emellertid ansett att meddelandens identifieringsuppgifter samt möjligheten att sammanställa och kombinera dem likväl i praktiken kan vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde

[45] RP 309/1993 rd, s. 53
[46] RP 309/1993 rd, s. 53-54, GrUU 28/2000 rd, s. 3, GrUU 30/2001 rd, s. 2, GrUU 54/2001 rd, s. 4, GrUU 13/2003 rd, s. 4-5, GrUU 9/2004, s. 2, GrUU 59/2006 rd, s. 2, GrUU 23/2006 rd, s. 2-3, GrUU 11/2005 rd, s. 4, GrUU 10/2004 rd, s. 4, GrUU 9/2004 rd, s. 4, GrUU 37/2002 rd, s. 3, GrUU 26/2001 rd, s. 3, GrUU 5/1999 rd, s.7, GrUU 26/1998 rd, s. 2-3, GrUU 7/1997 rd, GrUU 47/1996 rd.
[47] RP 309/1993 rd, s. 53, GrUU 11/2005 rd, s. 4, GrUU 36/2002 rd, s. 6, GrUU 2/1996 rd, GrUU 5/1999 rd, s. 4.
[48] RP 309/1993 rd, s. 54.
[49] GrUU 6/2012 rd, s. 3-4, GrUU 67/2010 rd, s. 4, GrUU 66/2010 rd, s. 7, GrUU 62/2010 rd, s. 4, GrUU 29/2008 rd. s. 2, GrUU 3/2008 rd, s. 2, GrUU 59/2006 rd, s. 2, GrUU 23/2006 rd, s. 2-3, GrUU 11/2005 rd, s. 4, GrUU 10/2004 rd, s. 4, GrUU 9/2004 rd, s. 4, GrUU 37/2002 rd, s. 3, GrUU 26/2001 rd, s. 3, GrUU 5/1999 rd, s. 7, GrUU 26/1998 rd, s. 2-3, GrUU 7/1997 rd, GrUU 47/1996 rd.

inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är.[50]

Det regelverk som ingriper i skyddet av identifikationsuppgifternas hemlighet ska uppfylla de allmänna förutsättningarna för att begränsa de grundläggande fri- och rättigheterna[51]. I grundlagsutskottets praxis har det utgående från detta ansetts möjligt att erhållandet av identifikationsuppgifter vid brottsutredning inte ska bindas vid vissa brottstyper, om regleringen i övrigt uppfyller de allmänna förutsättningarna för att begränsa de grundläggande rättigheterna.[52] Regleringen bör härvid dock begränsas till att gälla brott av den typ som äventyrar individens eller samhällets säkerhet eller hemfriden eller till brott som till sin grovhet kan jämföras med dem.[53]

6.1.2.5 Åtgärder för att realisera dataskyddet

En situation som kan anses stå tekniskt nära datatrafikspaning ingår i bestämmelsen i 272 § i informationssamhällsbalken. I bestämmelsen är det fråga om åtgärder för att förverkliga dataskyddet och den ger teleföretag, tjänsteleverantörer och sammanslutningsabonnenter rätt att bl.a. automatiskt analysera innehållet i alla de meddelanden som rör sig ut från nätet hos sammanslutningen i fråga eller kommer in i nätet. Enligt 3 mom. i bestämmelsen:

> ”Om det utifrån typen av meddelande, meddelandets form eller någon annan motsvarande omständighet är uppenbart att ett meddelande innehåller ett skadligt datorprogram eller ett skadligt kommando och uppnåendet av målen enligt 1 mom. inte kan säkerställas genom åtgärder som avses i 2 mom. 1 punkten *(automatisk analys av innehållet i meddelandet)*, får innehållet i ett enskilt meddelande behandlas manuellt. - -”

Bestämmelser om de syften för vilkas tryggande ovan nämnda åtgärder får vidtas finns i 1 mom. De intressen som ska tryggas verkar endast delvis anknyta till brottsbekämpning.
Syftena är att:

> ”1) upptäcka, förhindra och utreda störningar som kan inverka menligt på informationssäkerheten i kommunikationsnäten eller tjänster som anslutits till dem samt i informationssystemen och göra störningarna föremål för förundersökning,
> 2) trygga kommunikationsmöjligheterna för den som sänder eller tar emot meddelanden eller

[50] GrUU 18/2014 rd, s. 6
[51] GrUU 62/2010 rd, s. 4-5, GrUU 23/2006 rd, s. 3, GrUU 7/1997 rd
[52] GrUU 29/2008 rd, s. 2, GrUU 11/2005 rd, s. 4, GrUU 9/2004 rd, s. 4, GrUU 26/2001 rd, s. 3, GrUU 37/2002 rd, s. 3, GrUU 7/1997 rd
[53] GrUU 66/2010 rd, s. 7, GrUU 67/2010 rd, s. 4.

> 3) förhindra i 37 kap. 11 § i strafflagen avsedd förberedelse till sådana betalningsmedelsbedrägerier som planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna.”

Ursprungligen togs denna reglering in i lagen om dataskydd vid elektronisk kommunikation (20 §) som föregick informationssamhällsbalken år 2004. I innehållet i ett förtroligt meddelande fick man då ingripa endast utgående från i bestämmelsen nämnda brottsmisstankar (orsakande av fara för databehandlingen och störning av datatrafiken).

Enligt grundlagsutskottets utlåtande om den dåvarande regleringen var den bärande principen med regleringen att i kommunikationens samtliga parters intresse garantera fungerande och säkra datanät och på så sätt skapa förutsättningar för yttrandefrihet och skydd för kommunikationen på nätet. De omständigheter som syftar till att främja och trygga de grundläggande fri- och rättigheterna var enligt grundlagsutskottet godtagbara och tungt vägande skäl för begränsningar i den elektroniska kommunikationen på nätet. Ingrepp i förtroliga meddelanden fick inte göras annat än vid misstanke om brott som det sades i bestämmelsen. Det kunde betraktas som en risk för den enskildes och samhällets säkerhet i vid bemärkelse, om någon äventyrade datakommunikationerna och datasäkerheten. I detta givna sammanhang medförde bestämmelsen, enligt utskottet, inga problem med avseende på skyddet för förtroliga meddelanden i 10 § i grundlagen.[54]

Bestämmelsen ändrades år 2008. Då avstod man ifrån att ingripandet i ett meddelandes innehåll binds enbart till brottsrekvisitet. Enligt detaljmotiveringen till bestämmelsen (RP 48/2008 rd) följer av det att ingripande i innehållet i ett meddelande binds till brottsrekvisitet att en analys endast kan göras när en gärning är avsiktlig. I praktiken sänds inte skadliga meddelanden alltid med avsikt. För att dataskyddet ska kunna upprätthållas måste man kunna analysera också skadliga meddelanden som sänts oavsiktligt och som orsakar en risk för dataskyddet. Vidare konstateras det i förarbetet att det finns ett behov att manuellt behandla innehållet i ett enskilt meddelande, om det är uppenbart att man inte med hjälp av automatisk databehandling kan trygga att de mål som avses i det föreslagna 1 momentet realiseras. Grundlagsutskottet har medverkat till att både 20 § i den gamla lagen (GrUU 29/2008 rd), som informationssamhällsbalken upphävde, och informationssamhällsbalken stiftades (GrUU 18/2014).

6.1.3 Eventuella riktlinjer för nationell datatrafikspaning

De internationella människorättsfördrag som förpliktar Finland tillåter under vissa villkor underrättelse i fråga om både intern och gränsöverskridande datakommunikation. I beskrivningen av nuläget i betänkandet har det konstaterats att de allvarligaste hoten mot Finlands nationella säkerhet i första hand är utifrån kommande. Till följd av

[54] GrUU9/2004 rd, s. 4

detta anknyter Finlands behov till underrättelse som gäller den gränsöverskridande datakommunikationen.

I datatrafikspaning är det fråga om en underrättelsebefogenhet vars syfte det skulle vara att samla in underrättelseinformation om utländska aktörer och förhållanden som är nödvändig för den nationella säkerheten och produceras som stöd för den högsta statsledningens beslutsfattande. Vidare ska syftet vara att upptäcka och identifiera allvarliga hot utifrån som riktar sig mot den nationella säkerheten och samla in sådan information om dem som gör det möjligt att utforma en lägesbild, vidta avvärjningsåtgärder samt för militärmyndigheternas del ge en förvarning. Underrättelse är inte verksamhet som är person- eller brottsbunden på samma sätt som förebyggandet av brott. Föremål för datatrafikspaningen ska vara verksamhetssätt av mera allmän art än de kriminella gärningar som avses i strafflagen.

Som en central förutsättning för att datatrafikspaningen ska vara samhälleligt acceptabel kan anses att de hot som informationsinhämtningen får gälla definieras så klart och snävt som möjligt. Inte heller enligt de internationella människorättsfördragen får datatrafikspaningen vara en metod att inhämta information om vilket som helst hot eller vilken som helst risk. I jämförelseländerna har de hot och situationer som spaningen får gälla i allmänhet räknats upp i lag.

De hot som ska identifieras med hjälp av datatrafikspaning ska vara tillräckligt allvarliga och riktade mot säkerhetsintressen som är viktiga med tanke på den nationella säkerheten. Hoten kan till sin art vara antingen militära eller civila. Tillräckligt allvarliga hot mot den nationella säkerheten kan vara t.ex. militära hot, terrorism och med dessa jämförbar verksamhet samt spioneri som riktas mot Finland. För att spioneri ska kunna upptäckas och identifieras bör datatrafikspaning kunna användas oberoende av om den riktas mot staten eller den privata sektorn. Med hjälp av datatrafikspaning bör det vara möjligt att kartlägga källorna till ett hot och de verksamhetssätt som främmande stater använder i sitt spioneri.

Internationell organiserad brottslighet ska kunna omfattas av datatrafikspaning till den del som den äventyrar den nationella säkerheten. Likaså bör datatrafikspaning kunna användas för att inhämta information som behövs för att spridningen av massförstörelsevapen ska kunna förhindras.

Internationella krishanteringsinsatser har blivit mera krävande och denna utveckling kan antas fortsätta också i framtiden. Säkerheten vid krishanteringsinsatserna kunde förbättras med hjälp av den information som fås från datatrafikspaningen. Datatrafikspaning bör kunna användas för att upptäcka allvarliga hot som riktas mot kritisk infrastruktur. Dylika hot kan också komma via datanäten.

Främmande staters planer, avsikter och åtgärder kan i vissa fall skada eller äventyra Finlands utrikes- och säkerhetspolitiska intressen. Med hjälp av datatrafikspaning

kunde man i dessa situationer försäkra sig om att den högsta statsledningen får tillräcklig och tillförlitlig information i rätt tid.
I vissa situationer kan statens inre hot vara så allvarliga och ha sådana verkningar att de kan jämställas med de hot som behandlas ovan, och om dessa kunde man få information med hjälp av spaning som riktas mot gränsöverskridande datakommunikationsförbindelser. I fråga om ett dåd som till sina verkningar är tillräckligt allvarligt kan det hänvisas till massmördandet i Norge år 2011.
I kapitel 6.1.2 ovan behandlas begreppet nationell säkerhet i skenet av europeiska människorättskonventionen. Enligt arbetsgruppens uppfattning hör hot av ovan nämnt slag till området för begreppet nationell säkerhet på det sätt som t.ex. Europeiska människorättsdomstolen har tolkat begreppet.

Syftet med spaningen ska vara att upptäcka, identifiera och skaffa information om hoten. Däremot kan spaningen inte förhindra att hot realiseras. Kontaktytan mellan spaning och avvärjande åtgärder måste organiseras särskilt. Utgående från den information som erhålls genom spaning måste den behöriga myndigheten kunna vidta nödvändiga åtgärder för att avvärja ett hot. I det fortsatta arbetet ska det övervägas i vilken omfattning och på vilket sätt underrättelseinformationen kunde överlåtas så att den kunde användas t.ex. för att förebygga ett brott.

De internationella människorättsfördragen verkar inte ställa något kategoriskt hinder för användningen av datatrafikspaning för att reda ut brott. Det torde kunna anses klart att datatrafikspaning inte kan vara en vanlig metod för att undersöka nätbrottslighet eller annan massbrottslighet. Som utgångspunkt kunde tas att datatrafikspaning inte alls kan användas som en brottsundersökningsmetod. För detta torde det finnas skäl som anknyter till både individens rättsskydd och det faktum att metoderna för datatrafikspaning bör hållas hemliga.

En omständighet som är åtskild från den egentliga användningen av datatrafikspaning i brottsundersökningssyfte är att i samband med verksamheten sådana uppgifter kan komma till underrättelsemyndighetens kännedom som antyder att ett brott har begåtts. Om det är frågan om ett särskilt allvarligt brott, bör det övervägas på vilket sätt informationen kan ges till förundersökningsmyndigheten. Inte heller i detta fall ska det få vara fråga om att använda uppgifterna i rättsprocessen utan om att rikta in brottsundersökningen.

Om man i samband med datatrafikspaning upptäcker allvarliga cyberdåd som riktar sig mot den privata sektorn, bör man överväga på vilket sätt man kunde meddela dessa till det företag som är föremål för dåden. Målet ska vara att minimera de skador som näringslivet och samhällsekonomin orsakas.

Vidare har det i arbetsgruppen tagits upp att det finns ett behov att analysera datakommunikationsflödet också för att säkerställa att datatrafikspaningen är selektiv och för att följa med den teknologiska utvecklingen. Det ska vara fråga om att trygga

funktionsförmågan hos systemet för datatrafikspaningen. I det fortsatta arbetet bör det granskas om och i vilken omfattning en sådan verksamhet är möjlig att ordna med beaktande av de internationella människorättsfördragen samt kraven i grundlagen.

6.1.4 Realiseringen av datatrafikspaning

Datatrafikspaningen bör genomföras så att ur flödet av datakommunikation så effektivt som möjligt kan gallras fram den kommunikation som är väsentlig med tanke på spaningsuppdraget och förhindras att sådan kommunikation som inte ingår i uppgiften blir föremål för analysering.

Enligt europeiska människorättsdomstolen måste av lagen tillräckligt klart framgå i vilka förhållanden och under vilka förutsättningar medborgarna kan bli föremål för observation som myndigheterna utför i hemlighet. Dessutom förutsätter EUD:s dom i fallet Data Retention att behandlingen av personuppgifter begränsas på förhand. Dessa villkor ska beaktas när det övervägs om datatrafikspaning ska genomföras.

I datakommunikationen måste man kunna avskilja de uppgifter som är av betydelse med tanke på den nationella säkerheten. Ett sätt att uppfylla kraven är att använda sökbegrepp, som har definierats tillräckligt exakt på förhand, eller beskrivningar i ord av den verksamhet som äventyrar den nationella säkerheten och som så konkret som möjligt karaktäriserar föremålet för informationsinhämtningen. Dessa ska användas för att inrikta spaningsverksamheten.

Föremål för beskrivningen ska vara sådana kommunikationsmässiga och andra verksamhetsmodeller som man vet eller som man kan anta att har samband med verksamhet som äventyrar den nationella säkerheten. Verksamheten kunde t.ex. organiseras så att den myndighet som behandlas i avsnitt 6.1.6 godkänner beskrivningen som grund för datatrafikspaning, vilket kan anses uppfylla kravet på avgränsning på förhand. Utgående från beskrivningen ska den myndighet som svarar för datatrafikspaningen utforma de sökbegrepp som är nödvändiga för att informationsinhämtningen ska kunna riktas rätt. Användningen av de sökbegrepp som myndigheten har utformat ska dokumenteras på ett täckande sätt, vilket gör det möjligt att i efterhand övervaka verksamheten.

De sökbegrepp som ska användas i den första fasen av datatrafikspaningen ska kunna vara identifieringsuppgifter. Dessa är individualiseringsuppgifter som beskriver t.ex. nätanordningar och nätadresser samt t.ex. uppgifter som beskriver tid och plats för kommunikationen. För att man ska få tillräckliga uppgifter om de hot som är föremål för datatrafikspaningen, ska man i fråga om den kommunikation som gallrats fram utifrån sökbegrepp också kunna reda ut innehållet.

När syftet med datatrafikspaningen är att upptäcka datanätsspioneri som utförs med hjälp av skadeprogram, bör också sökbegrepp som gäller innehållet kunna användas i

ett exceptionellt fall genast i första fasen. Sökbegrepp ska då vara teknisk skadeprogramsidentifikation och handlingsmodellen ska vara densamma som i den verksamhet om vilken bestäms i 272 § i informationssamhällsbalken.

En begränsning av integritetsskyddet ska kunna lindras på så sätt att gallringen enligt sökbegrepp i första fasen görs maskinellt. Med hjälp av sökbegrepp ska man på ett ändamålsenligt sätt från kommunikationens totala massa kunna skilja ut de uppgifter som är väsentliga med tanke på spaningsuppdraget. Uppgifterna ska kunna bli föremål för manuell behandling först efter en maskinell gallring. Med tanke på integritetsskyddet är det väsentligt att ett sådant meddelande eller identifieringsuppgifterna till ett sådant meddelande som inte motsvarar sökbegreppen inte slinker med i den manuella behandlingen.

Datatrafikspaning, så som den beskrivs ovan, ska vara en process som består av flera på varandra följande arbetsfaser, där den kommunikationsmängd som är föremål för behandlingen hela tiden blir mindre i takt med att processen framskrider. Då ska endast de kommunikationsuppgifter sparas som har genomgått varje fas av processen. Övriga uppgifter ska förstöras, och efter att de förstörts ska de inte längre kunna sökas fram av myndigheterna. De internationella människorättsförpliktelser som binder Finland förutsätter att klara förfaringssätt skapas för behandlingen av uppgifterna.

Datatrafikspaningen begränsar i sina olika faser i olika omfattning skyddet för ett konfidentiellt meddelande. I den första fasen av datatrafikspaningen ska sökbegreppen jämföras med alla de meddelanden som rör sig i de datakommunikationsflöden som valts som objekt. Också den övervägande delen av datakommunikationen som inte är av betydelse för den nationella säkerheten ska vara föremål för en automatiskt utförd jämförelse. I denna fas kan jämförelsen grunda sig på identifieringsuppgifterna gällande annan datakommunikation än skadeprogramstrafiken. Jämförelsen ska göras automatiserat och de meddelanden som inte motsvarar sökbegreppen ska inte komma till den manuella behandlingen. Graden av exakthet i de sökbegrepp som ska användas automatiskt i verksamheten inverkar på risken för om även sådan kommunikation som ska anses vara sidokommunikation gallras ut för att bli föremål för den manuella fortsatta behandlingen. Ju mera exakta sökbegreppen är, desto mindre är risken för att sådan information som är oväsentlig med tanke på spaningsuppdraget filtreras fram för fortsatt behandling.

Nästa fas av processen i datatrafikspaningen ska innehålla en mera djupgående begränsning av den konfidentiella kommunikationen, men den ska gälla en väsentligt snävare personkrets. Den kommunikation som filtrerats fram utgående från de sökbegrepp som används ska då tas till föremål för manuell analysering. Den datakommunikation som är föremål för den manuella behandlingen är i princip betydelsefull för spaningsuppdraget, och meddelandets innehåll ska vid behov kunna redas ut.

Organiserandet av datatrafikspaningen på det sätt som föreslås ovan förutsätter inte att identifieringsuppgifter sparas i stor skala, ospecificerat, långvarigt eller obegränsat utan det ska vara fråga om att datakommunikation filtreras utgående från sökbegrepp som har definierats på förhand och att uppgifter som är väsentliga för den nationella säkerheten sparas på grundval av detta.[55] De uppgifter som ska sparas kommer, även när det är fråga om den största volymen, att utgöra endast en bråkdel av den totala volymen av kommunikation som överskrider gränserna.

Organiserandet av datatrafikspaningen förutsätter att för teleföretag eller ägare av gränsöverskridande datakommunikationstrådar ställs en skyldighet att anvisa accesspunkter samt att ge de uppgifter som detta kräver till den myndighet som svarar för att datatrafikspaning genomförs. Genomförandet av spaningen får inte göra den allmänna datakommunikationen långsammare. En accesspunkt bör planeras i samarbete med teleföretagen så att de olägenheter detta medför för dem kan minimeras. Utgångspunkten är att de direkta kostnader som företagen eventuellt orsakas av den tekniska verksamheten ska täckas av de parter som genomför datatrafikspaningen.

6.1.5 Riktlinjer för det administrativa organiserandet av datatrafikspaning

Ovan i avsnitt 6.1.3 har de hot behandlats som det med tanke på den nationella säkerheten vore nödvändigt att inhämta information om genom datatrafikspaning. Enligt gällande lagstiftning ankommer det på olika myndigheter att följa med dessa hot. Informationsinhämtningen om militära hot ankommer på försvarsmakten, medan igen bevakningen av de hot av civil art som avses i betänkandet i huvudsak hör till skyddspolisen. Centralkriminalpolisen avvärjer internationell organiserad brottslighet. Enligt arbetsgruppens syn är det inte nödvändigt att ändra på arbetsfördelningen mellan myndigheterna.

Det är inte ändamålsenligt att de myndigheter som behöver underrättelseinformation var för sig utför datatrafikspaning, utan det är skäl att grunda verksamheten på en centraliserad lösning. I en centraliserad lösning ges en myndighet i uppdrag att sköta det tekniska genomförandet av datatrafikspaningen *(datatrafikspaningsmyndigheten)*, som på uppdrag av övriga myndigheter som är berättigade att få den information som datatrafikspaningen ger som resultat *(uppdragsgivarmyndigheter)* inhämtar de uppgifter genom datatrafikspaning som dessa behöver. För en centraliserad lösning talar de krav som ska ställas på att verksamheten ska vara harmoniserad och hållas hemlig, den specialisering och det tekniska kunnande som verksamheten kräver samt aspekter som sammanhänger med övervakningen av att verksamheten är lagenlig. EMD har förutsatt att för verksamheten skapas klara förfaranden samt en laglighetsövervakning som täcker dess lagenlighet. För dessa kan man bäst sörja i en centraliserad modell.

[55] GrU har i sitt utlåtande GrUU 18/2014 rd ansett att åtminstone sådant sparande av identifieringsuppgifter strider mot proportionalitetskravet.

Det tekniska utförandet av datatrafikspaningen måste vara myndighetsverksamhet. I verksamheten är det nödvändigt att behandla sådan sekretessbelagd information som, om den kommer ut i offentligheten, allvarligt äventyrar den nationella säkerheten.

Till datatrafikspaningsmyndighet vore det ändamålsenligast att utse en sådan myndighet som redan har den tekniska kunskap och de internationella relationer gällande underrättelsesamarbete som verksamheten förutsätter. Cybersäkerhetscentret, som deltar i avvärjningen av datanätshot, har det tekniska kunnande som verksamheten förutsätter. Centret har emellertid inte uppgifter med anknytning till inhämtandet av underrättelseinformation och följaktligen inte heller de samarbetsrelationer som underrättelseverksamheten förutsätter. Centralkriminalpolisen har internationella samarbetsrelationer. Den är emellertid den myndighet som svarar för att de brott som hör till dess verksamhetsområde reds ut och den sörjer för det tekniska genomförandet av teletvångsmedel som anknyter till polis- och tvångsmedelslagen för en brottsprocess. Skyddspolisen har internationellt samarbete med anknytning till inhämtandet av underrättelseinformation. Försvarsmaktens underrättelsetjänst har både den tekniska kunskap som verksamheten förutsätter och de internationella samarbetsrelationer som underrättelseverksamheten förutsätter.

Datatrafikspaningsmyndigheten ska få sina uppdrag av uppdragsgivarmyndigheterna. Som uppdragsgivarmyndigheter kommer de myndigheter i fråga som svarar för avvärjningen av de hot som är föremål för underrättelsen. Sådana är försvarsmakten, Skyddspolisen och Centralkriminalpolisen.

Om man i det fortsatta arbetet stannar för en lösning där det tekniska utförandet av datatrafikspaningen ges en verksamhetsenhet som hör till försvarsmakten, måste även om dess uppdrag att bistå civila myndigheter och om civila myndigheters uppdragsgivarbefogenhet gentemot centret föreskrivas i lag.

Enligt arbetsgruppens uppfattning har även Finlands högsta statsledning ett behov att få den information som inhämtas genom datatrafikspaningen. Därför ska också den högsta statsledningen ha en möjlighet att ge datatrafikspaningsmyndigheten uppdrag. Uppdragen ska emellertid kanaliseras till den som tekniskt utför datatrafikspaningen via de myndigheter som svarar för att hot avvärjs.

6.1.6 Omständigheter som ska beaktas med tanke på rättsskyddet

När datatrafikspaning eventuellt organiseras bör respekten för de grundläggande fri- och rättigheterna och de mänskliga rättigheterna, proportionalitetsprincipen, principen om minsta olägenhet och principen om ändamålsbundenhet beaktas som styrande principer.

Tillståndsförfarandet

EMD har ansett det viktigt att den informationsinhämtande myndigheten inte har obegränsad prövningsrätt när det gäller att inrikta informationsinhämtandet. Ett sätt att begränsa myndighetens prövningsrätt är att föreskriva om att tillstånd ska sökas hos en utomstående part för varje enskilt spaningsuppdrag.
Enligt EMD ska området för tillståndsprövningen framgå av lagen. Väsentligt i fråga om detta är att det i tillståndsansökan och i tillståndet tillräckligt exakt kan visas vilka persongrupper spaningen riktas mot. En tillståndsprövning som grundar sig på godkännandet av antingen de sökbegrepp som ska användas i gallringen eller en eventuell exakt beskrivning av den verksamhet eller de personer som äventyrar den nationella säkerheten kan anses uppfylla kraven ovan.

EMD har förutsatt att om tillståndets giltighetstid föreskrivs i lag. EMD har i sitt avgörande *Weber & Saravia mot Tyskland* ansett att en tidsfrist på tre månader är förenlig med proportionalitetsprincipen.

Såsom det framgår av den internationella jämförelsen varierar det mellan de olika jämförelseländerna vilken part som beviljar tillstånd. En särskild för detta ändamål grundad domstol eller en politiskt ansvarig part kan bevilja tillstånd. Det vore förenligt med det finska rättssystemet att tillståndsprövningen skulle vara juridisk till sin art. När tillståndsförfarandet ordnas bör sekretessfaktorer, behovet av specialkunnande som frågorna kräver samt säkerställandet av individens rättsskydd beaktas. Till exempel i Sverige övervakas en privatpersons intresse i tillståndsförfarandet av en offentlig ombudsman. Möjligheterna att anföra besvär i tillståndsförfarandet måste bedömas. Likaså bör det bedömas om ett förenklat tillståndsförfarande kunde användas i situationer då det är bråttom.

Om behandlingen av informationen

EMD har ansett[56] att på lagnivå måste det föreskrivas tillräckligt exakt om det förfarande som ska följas vid datatrafikspaning. Bestämmelserna om förfaringssättet bör gälla åtminstone granskning, utnyttjande, förvaring, överlåtelse och förstöring av informationen.

Med granskning av uppgifterna avses manuell behandling av de uppgifter som filtrerats fram automatiskt på grundval av sökbegrepp. Riktlinjerna för i vilka situationer filtrerade uppgifter kan bli föremål för manuell behandling behandlas i avsnitt 6.1.4. Likaså har utnyttjandet av uppgifter vid avvärjningen av hot och vid informerandet av den högsta statsledningen behandlats i avsnitt 6.1.3.

[56] Liberty and others v. Förenade konungadömet samt Weber & Saravia v. Tyskland

De uppgifter som uppkommer som resultat av datatrafikspaning är delvis personuppgifter. Enligt grundlagen måste bestämmelser finnas på lagnivå om behandlingen av personuppgifter hos uppdragsgivarmyndigheten samt hos datatrafikspaningsmyndigheten. Enligt 10 § 1 mom. i grundlagen föreskrivs om skydd av personuppgifter närmare genom lag.

Vid överlåtelsen av uppgifter ska det i en bassituation vara fråga om överlåtelse till uppdragsgivarmyndigheten av uppgifter som datatrafikspaningsmyndigheten har inhämtat. Utöver detta bör det övervägas under vilka förutsättningar uppgifter kunde överlåtas till utomstående parter. Sådana är t.ex. företag som har blivit föremål för en allvarlig datanätsattack som upptäckts vid datatrafikspaningen. Vid övervägningen måste de begränsningar i behandlingen av personuppgifter som följer av lagstiftningen beaktas.

I lagen bör finnas bestämmelser om förutsättningarna för att underrättelseinformation ska kunna överlåtas till internationella samarbetsparter. Utgångspunkten ska vara att överlåtelsen av uppgifterna främjar den nationella säkerheten och inte äventyrar Finlands intressen, inklusive samhällsekonomiska intressen.

Vid spaningen kan man också få information som inte anknyter till det uppdrag som spaningen gäller. I sina avgöranden har EMD behandlat frågan om användningen av s.k. överskottsinformation. Av praxis i fråga om avgörandena kan man dra den slutsatsen att det behövs en tillräckligt täckande och exakt reglering av hur dylik information får användas. Även om avgörandena gäller brottsbekämpning, torde man av dem också kunna sluta sig till hur behandlingen av sådan information bör ordnas i underrättelseverksamheten. Det bör vara möjligt att använda överskottsinformation åtminstone då informationen gäller ett sådant hot för vilket datatrafikspaning hade fått användas. Överlåtelse av information till förundersökningsmyndigheten för att inrikta undersökningen har behandlats särskilt i avsnitt 6.1.3.

Frågan om förstöring av information måste granskas särskilt i fråga om information som stämmer överens med uppdraget, överskottsinformation som är av betydelse för den nationella säkerheten och överskottsinformation som inte har något samband med den nationella säkerheten. I fråga om information som stämmer överens med uppdraget ska förvaringstider fastställas samt hur de fastställs och hur förvaringsskyldigheten fördelas mellan datatrafikspaningsmyndigheten och uppdragsgivarmyndigheten. Förvaringen och förstöringen av överskottsinformation som är av betydelse för den nationella säkerheten ska fastställas på samma grunder.

Överskottsinformation som inte har något samband med den nationella säkerheten bör förstöras omedelbart sedan det har upptäckts att den är sådan.

Med datatrafikspaning har man inte för avsikt att bevaka datakommunikationen mellan parter som vistas i Finland. Inte heller sådant sparande i en molntjänst utomlands

som görs från Finland och i vilket inte ingår kommunikation har man för avsikt att bevaka, med undantag av skadeprograms kommunikation. I det fortsatta arbetet ska det sörjas för tillräckliga bestämmelser för att säkerställa att sådan information förstörs omedelbart när den har upptäckts.

Rättsmedel

I det fortsatta arbetet bör det övervägas hurdana rättsmedel som bör fogas till datatrafikspaningen. Sådana kan vara klagomål, indirekt granskningsrätt på begäran av en person gällande lagenligheten i behandlingen av personuppgifter och den offentliga ombudsmannens deltagande i behandlingen av en tillståndsansökan. Det bör också övervägas om det bör finnas en besvärsmöjlighet i fråga om tillståndsbeslutet och hur denna i så fall kunde förverkligas.

Övervakning

Enligt EMD:s avgörandepraxis bör övervakningen av myndigheternas hemliga observationsbefogenheter ordnas effektivt. Övervakningen kan inte endast vara intern övervakning som görs av myndigheten själv. Inte heller laglighetsövervakning utförd av ett oberoende organ kan ensam anses ge tillräckliga garantier för rättsskyddet, om inte inom ramen för den fattas bindande beslut som kan överklagas. Enligt EMD är det av betydelse att det finns både utomstående domstolsövervakning och parlamentarisk övervakning.

Enligt grundlagen är den behörighet att övervaka myndighetsverksamhetens lagenlighet som statsrådets justitiekansler och riksdagens justitieombudsman har allmän. Dataombudsmannen övervakar att behandlingen av personuppgifter är lagenlig. Övervakningen av datatrafikspaning kan förutsätta sådan specialisering att också grundandet av ett externt specialövervakningsorgam bör övervägas. Dessutom bör det sörjas för datatrafikspaningsmyndighetens och uppdragsgivarmyndigheternas interna laglighetsövervakning samt sådan övervakning som de styrande ministerierna utför. Datatrafikspaningen bör övervakas också parlamentariskt. EMD har konstaterat att riksdagens deltagande i övervakningen av hemliga observationsbefogenheter är av betydelse med tanke på skyddandet av demokratin.

6.1.7 Konsekvensbedömning av datatrafikspaningen

Vägning av för- och nackdelarna med datatrafikspaning

När det övervägs hur godtagbar datatrafikspaning är måste det bedömas om den nytta som verksamheten medför för den nationella säkerheten är större än den nackdel som verksamheten eventuellt orsakar integritetsskyddet samt samhällsekonomin och företagen.

De hot som kan identifieras med hjälp av datatrafikspaning är internationella, allvarliga och riktar sig mot statens viktiga säkerhetsintressen. Med hjälp av datatrafik-

spaning ska man åstadkomma information om utländska aktörer och omständigheter som är av betydelse med tanke på den nationella säkerheten och som ges som stöd för den högsta statsledningens beslutsfattande.
Av den internationella jämförelse som ingår i betänkandet samt av öppna källor[57] framgår att datatrafikspaning används i flera västländer. Det är uppenbart att det i dessa länder anses som en effektiv metod att inhämta information. Också de utländska experter som arbetsgruppen har hört konfidentiellt har betonat att datatrafikspaning är ett sätt att få information som är nödvändig för att de hot som riktar sig mot den nationella säkerheten ska kunna avvärjas och för att inhämta strategisk information som grund för statens högsta beslutsfattande. Vid hearingarna togs det upp att ett modernt utrikes- och säkerhetspolitiskt beslutsfattande endast kan grunda sig på tidsenlig underrättelseinformation till vilken datatrafikspaningen bidrar med en viktig del.

Datatrafikspaningen skulle också på ett betydande sätt komplettera Finlands möjligheter att skydda sig mot allvarliga datanätshot. De nuvarande systemen upptäcker inte statliga spionageprogram och andra skadliga program, vilka har en särskilt stor skadlig effekt på den nationella säkerheten. Även näringslivet skulle ha nytta av datatrafikspaning när det skyddar sig mot de allra allvarligaste datanätshoten.

Å andra sidan är det klart att systemet begränsar skyddet för ett konfidentiellt meddelande som har tryggats som en grundläggande rättighet. I avsnitt 6.1.4 i betänkandet behandlas på vilket sätt datatrafikspaning kunde ordnas så att det i så liten mån som möjligt begränsar integritetsskyddet och är godtagbart med tanke på de internationella människorättsfördragen. Med tanke på grundlagsskyddet av ett förtroligt meddelande tycks genomförandet av datatrafikspaning trots detta vara problematiskt.

Datatrafikspaning ska funktionellt jämställas med de verksamhetsrättigheter som aktörerna i informationssamhället redan nu kan använda för att sörja för sitt dataskydd. I båda är det fråga om automatisk filtrering av kommunikationen på grundval av sökbegrepp. Till manuell behandling av ett meddelande kan man övergå i det fall att det är uppenbart att det finns en motsvarighet mellan innehållet i meddelandet och det sökbegrepp som använts. Ett oberoende tillståndsförfarande och övervakning bör fogas till datatrafikspaningen.

Vid hearingar har det tagits upp att det av tekniska skäl inte i alla situationer är möjligt att skilja åt utländsk och inhemsk datatrafik. Följaktligen kan begränsningen av skyddet för ett konfidentiellt meddelande i princip också rikta sig mot inhemsk datakommunikation. Skyddet för ett konfidentiellt meddelande ska i dylika situationer kunna sörjas för t.ex. med hjälp av ett förbud att behandla inhemsk datakommunikation och en skyldighet att omedelbart stryka dessa uppgifter.

[57] Se t.ex. Europaparlamentets undersökning ”National programmes for mass surveillance of personal data in EU member states and their compatibility with EU law” (http://www.europarl.europa.eu/studies).

Med tanke på skyddet för ett förtroligt meddelande ska det beaktas att förhållningssättet till identifieringsuppgifter och till att de kan komma att röjas kanske håller på att förändras. I avsnitten 6.1.2.3 och 6.1.2.4 i betänkandet har EUD:s s.k. Data Retention -dom och grundlagsutskottets påpekanden om den granskats. Det måste säkerställas att det vid datatrafikspaningen inte sparas identifikationsuppgifter i stor skala, ospecificerat, långvarigt och obegränsat. I datatrafikspaningen bör sådana uppgifter med anknytning till gränsöverskridande datakommunikation kunna sparas som motsvarar de sökbegrepp som använts och som därmed kan bedömas vara av betydelse när hot mot den nationella säkerheten avvärjs. Även när de är som mest kommer de uppgifter som sparas att utgöra endast en bråkdel av all den kommunikation som överskrider gränserna.

Utöver verkningarna på medborgarna ska det också bedömas vilka verkningar datatrafikspaning har på företagen och på näringslivet som helhet.

Vid hearingarna har det tagits upp att datatrafikspaningen kan ha negativa verkningar på Finlands internationella konkurrenskraft samt på Finlands attraktion som investeringsobjekt. I dessa utlåtanden har det ansetts att Finlands attraktion som investeringsobjekt grundar sig på rena datanät och på Finlands rykte som ett land med högt dataskydd.

Bedömningen att datanäten är rena ifrågasätts i Cybersäkerhetscentrets rapport[58] enligt vilken i de västländer som systematiskt bevakar cyberattacker årligen upptäcks tiotals cyberspionfall, där som tekniska hjälpmedel har använts ett riktat skadeprogram. Enligt rapporten gäller hotet också Finland. Avvikande från dessa länder har Finland i dagens läge inget system med vilket särskilt allvarliga riktade skadeprogramsattacker kunde bevakas. Således kan det bedömas att uppfattningen om särskilt rena datanät åtminstone i fråga om allvarligare cyberdåd grundar sig på bristfällig nationell förmåga att upptäcka sådana. Det kan bedömas att utvecklandet av förmågan till datatrafikspaning i Finland höjer tröskeln för att rikta cyberspioneri mot vårt land.

Påståendet att datatrafikspaning har en försvagande inverkan på det höga dataskyddet i Finland bör bedömas mot de riktlinjer som beskrivs ovan för denna verksamhet. Datatrafikspaningen kommer, om den blir av, att inriktas på den datakommunikation som överskrider den finska gränsen. Största delen av de länder till vilka Finlands nuvarande och planerade datakommunikationsförbindelser går, kan redan nu bevaka den datakommunikation som går genom deras territorier utgående från sin egen lagstiftning. Detta innebär att den datakommunikation som går genom de finska internationella nätförbindelserna redan nu kan vara föremål för övervakning och spaning av andra än landets egna myndigheter.

[58] Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti. (Hotet från riktade skadeprogramsattacker måste tas på allvar) Kommunikationsverkets Cybersäkerhetscenters rapport. Hösten 2014

Arbetsgruppen har strävat efter att reda ut vilka negativa verkningar lagstiftning om datatrafikspaning eventuellt kan ha på investeringar. Det är svårt att bedöma verkningarna för Finlands del. Arbetsgruppen har inte fått kännedom om några undersökningar i saken. Ett exempel på ett land som under de senaste åren har lagstiftat i detalj och offentligt om datatrafikspaning är Sverige.

Försvarsministeriet beställde en utredning av Gearshift Group Oy för att reda ut vilka eventuella konsekvenser för investeringarna Sveriges signalspaningslag, den s.k. FRA-lagen, har haft. Föremål för utredningen var ICT-sektorns investeringar i Sverige och Finland under åren 2008–2013. I utredningen utnyttjades utöver egentliga forskningskällor, information ur marknadsundersökningscentrens rapporter samt sakkunnigas utvärderingar som hittades i medierapporter. I sin helhet ingår utredningen som bilaga 1 till betänkandet. Resultaten av utredningen presenteras i korthet nedan:

> *Konsekvenser för investeringarna och förutsättningarna för dem.* I utredningen upptäcktes inget sådant avvikande i den allmänna utvecklingen av de utländska investeringarna som kunde förklaras med inverkan från FRA-lagen. Enligt utredningen har lagens ikraftträdande ingen klar betydelse för utvecklingen i de utländska investeringar som riktas till Sverige jämfört med dem som riktas till Finland och Danmark.
>
> *Konsekvenser för FoU-verksamheten i Sverige.* De svenska forsknings- och utvecklingsutgifterna i relation till BNP sjönk något från 2009 framåt, men nedgången i nivån på utvecklingsutgifterna är svår att relatera just till FRA-lagen, eftersom den globala ekonomiska recessionen infaller under denna period. Å andra sidan, när man granskar utvecklingen i fråga om finansieringskällorna, kan man upptäcka att de utländska parterna till och med klart har ökat sina satsningar i relation till satsningarna från både den privata och den offentliga sektorn i Sverige. Detta ger starka indicier på att FRA-lagen inte har haft någon betydelse när de utländska forsknings- och utvecklingssatsningarna har riktats.
>
> *Konsekvenser för Sveriges internationella konkurrenskraft.* I World Economic Forums jämförelser placerar Sverige sig bland topp tio i fråga om både internationell konkurrenskraft och innovationer. Särskilt med tanke på ICT-investeringar kan de olika ländernas konkurrenskraft bedömas via förutsättningarna för datacenterverksamheten. I Data Center Risk Index -jämförelsen år 2013 har Sverige bedömts vara det tredje bästa placeringslandet för datacenter, medan Finland igen i samma jämförelse har plats nio. Det bedöms att FRA-lagen inte har haft negativa verkningar med tanke på placeringen av datacenter. Sveriges konkurrenskraft ses i form av betydande nya datacenterprojekt, bl.a. Facebook 2011 och utvidgning av kapaciteten 2014, KnC Miner 2014, Hydro66 2014 samt Bahnhofs stora utbyggnadsprojekt i Stockholm. Enligt utred-

ningen kan Sveriges klara underrättelselagstiftning i förhållandena efter det s.k. Snowden-fallet till och med ge en internationell konkurrensfördel. Vad gäller stora, långvariga investeringar är en minimering av riskerna och möjligheten att kunna förutse hur omgivningen utvecklas betydande faktorer som inverkar på ländernas konkurrenskraft.

Konsekvenser för uppkomsten av ny företagsverksamhet i Sverige och Finland. Sverige tar en klar topplacering vid en jämförelse av utvecklingen vad gäller grundandet av nya företag i Sverige, Finland och Danmark åren 2005 – 2012. Utredningen bedömer att betydelsen av FRA-lagen i företagens allmänna verksamhetsmiljö är mycket liten. Den bedöms inte ha inverkat på företagsverksamhetens utveckling eller på uppkomsten av nya företag.

I utredningens sammandrag konstateras det att FRA-lagens ikraftträdande inte har någon klar koppling till de utländska investeringarna i ICT-sektorn. Några skillnader till motsvarande investeringar i Finland, som skulle kunna förklaras med FRA-lagen, kunde inte konstateras i utredningen. Enligt utredningens bedömning skapar en exakt reglering av FRA-lagens typ en mera förutsebar omgivning för alla aktörer på ICT-sektorn.

Resultaten av utredningen stöds av de uppgifter arbetsgruppen fått vid sina hearingar. Enligt dem har FRA-lagen inte påverkat den svenska konkurrenskraften negativt och inte heller minskat mängden investeringar som riktar sig mot landet.

I fråga om datacenterinvesteringarna kan det ännu särskilt konstateras att enligt en utredning[59] som forskningsbolaget Gartner har publicerat i september 2014 upplevs Sverige och Norge som de mest attraktiva placeringsplatserna för datacenter. Underrättelselagstiftningarna i Sverige och Norge togs inte upp i undersökningen.

En klar lagstiftning skapar en förutsebarhet som är viktig när företagens verksamhet planeras och investeringsbeslut fattas. En exakt reglering kunde vara en internationell konkurrensfördel för Finland.

Näringslivet har bekymrat sig över att enskilda finska företags konkurrenskraft på den internationella marknaden blir sämre, om de åläggs att i samband med datatrafikspaning överlåta krypteringsnycklar eller installera bakdörrar i programvara eller anordningar. Arbetsgruppen föreslår inga sådana skyldigheter för näringsidkarna.

[59] Gartners utredning ”Save up to 50 % on European Colocation by Choosing the Right Location”, offentliggjordes 16.9.2014.

För att verksamheten ska kunna organiseras förutsätts att teleföretagen eller ägarna till gränsöverskridande datakommunikationstrådar åläggs att visa accesspunkterna för den myndighet som svarar för genomförandet av datatrafikspaningen.

Vid de hearingar som arbetsgruppen ordnade för intressegrupperna påpekades att den datatekniska utvecklingen kommer att minska effektiviteten i datatrafikspaningen i framtiden. Enligt dessa syner kommer detta centralt att påverkas av krypteringen av datakommunikation och de ökande mängderna datakommunikation.

Vid hearingarna togs det upp att till följd av utvecklingen i krypteringsteknikerna kommer det i framtiden inte att vara möjligt att öppna en kryptering utan krypteringsnyckel. Detta får konsekvenser för huruvida man kommer at få sådan information i realtid genom datatrafikspaning som behövs vid underrättelsen. Genom datatrafikspaningen kan man emellertid trots krypteringen få information som är av betydelse med tanke på den nationella säkerheten t.ex. utgående från identifikationsuppgifterna. Datatrafikspaning ska även användas för att upptäcka datanätsattacker, något som inte påverkas av eventuell kryptering. Enligt de tekniska experter som arbetsgruppen hört kan man säkerställa att systemet är tillräckligt effektivt utan att kräva att företagen ger krypteringsnycklar eller installerar bakdörrar.

Vid hearingarna ifrågasattes hur effektiv datatrafikspaningen är också på basis av det faktum att mängderna datakommunikation kommer att öka i framtiden. En ökning av datakommunikationsmängderna kan dock inte anses minska behovet av datatrafikspaning, utan snarare öka det. Det att hoten flyttar in i datanäten har behandlats i avsnitt 2 i betänkandet. De ökande mängderna datakommunikation måste kunna bemötas med tillräckliga resurser i verksamheten och med att man sörjer för att spaningsprocessen är tillräckligt selektiv.

Ett sammandrag av intressegruppernas och experternas ställningstaganden finns i bilaga 2 till betänkandet.

Ekonomiska verkningar och personalverkningar

Hur stora de ekonomiska verkningarna blir beror på, om man väljer en centraliserad eller decentraliserad modell för genomförandet av datatrafikspaningen. Om man vid genomförandet av datatrafikspaningen bestämmer sig för den centraliserade lösning som presenteras i betänkandet och som teknisk utförare utser en enhet som hör till försvarsmakten, inriktas resursverkningarna i första hand på försvarsmakten. Om grunderna för fördelningen av kostnaderna mellan de parter som deltar i verksamheten måste överenskommas närmare i det fortsatta arbetet.

En parlamentarisk utredningsgrupp, som rett ut utmaningarna på lång sikt för försvaret, konstaterar i sin rapport (Riksdagens kanslis publikation 3/2014) att den nuva-

rande finansieringsramen inte möjliggör tillräckliga resurser för att utveckla cybersäkerheten varken inom försvarsförvaltningen eller inom andra förvaltningsområden.

Genomförandet av datatrafikspaning förutsätter tilläggsresurser oberoende av på vilket sätt eller i vilken omfattning verksamheten organiseras. Det är framför allt fråga om systeminvesteringar och personalresurser.

Också uppdragsgivarna orsakas kostnader vid datatrafikspaning, t.ex. av analys- och översättningstjänster.

Eventuella tillståndsmyndigheter och övervakningsmyndigheter orsakas också kostnader, men dessa är det ännu i detta skede svårt att uppskatta.

6.2 Personbaserad underrättelseinhämtning utomlands och spaning i utländska datasystem

6.2.1 Allmänt

De allvarligaste hot som riktar sig mot den finska nationella säkerheten är så gott som utan undantag av internationellt ursprung eller åtminstone har de kopplingar till utlandet. Till följd av detta finns all information som påverkar säkerheten i det finska samhället inte tillgänglig i landet. Om man vill trygga samhället på ett framgångsrikt sätt, måste de finska säkerhetsmyndigheterna kunna inhämta information också om utländska aktörer.

Med underrättelse utomlands avses inhämtande av sådan information om utländska förhållanden och objekt som är väsentlig med tanke på den nationella säkerheten. Syftet med underrättelse utomlands är att samla in den information som är nödvändig för den högsta statsledningens säkerhetspolitiska beslutsfattande samt för avvärjningen av allvarliga yttre säkerhetshot.

Till följd av den karaktär som underrättelse utomlands har är verksamhetens globala utgångspunkt att man strävar efter att inhämta de uppgifter som behövs med så en så enkel metod som möjligt. I praktiken baserar sig underrättelsen ofta på handlingsmodeller som påminner om samverkan. Det är fråga om utbyte av information och synpunkter som sker på frivillig basis mellan myndigheterna i två stater och som båda parterna har nytta av. Informationsutbytet kan gälla t.ex. fenomen som är föremål för gemensamt intressen, enskilda händelser, iakttagelser eller politiska stämningar som den part som ger informationen erbjuder sin egen tolkning om och därmed strävar efter att påverka mottagarpartens syn. Utöver dylikt ömsesidigt informationsutbyte kan underrättelseverksamhet utomlands också grunda sig på ensidig verksamhet från den stats sida som utför underrättelsen. I en bassituation innehåller verksamheten det att den stat som utför underrättelse sänder personal utomlands som utgående från sin

tjänsteställning gör allmänna iakttagelser av förhållandena i stationeringslandet samt för diskussioner med representanter för eller medborgare i stationeringslandet. Även om det i detta fall inte är fråga om informationsutbyte som uttryckligen har överenskommits med stationeringslandet, sker verksamheten ofta med stationeringslandets tysta medgivande. Alla länder måste de facto till en viss gräns tåla underrättelse på sitt territorium.

I vissa situationer, som kan beskrivas som exceptionella, räcker det inte med det ovan beskrivna samarbetet eller underrättelse som grundar sig på ett tyst godkännande. I dylika fall borde information som är ytterst viktig med tanke på den finska nationella säkerheten kunna inhämtas med hjälp av hemliga underrättelsemetoder. Underrättelse utomlands med hjälp av hemliga metoder kan delas in i personbaserad underrättelseinhämtning utomlands och spaning i utländska datasystem.

Med personbaserad underrättelseinhämtning utomlands avses informationsinhämtning som baserar sig på personligt umgänge med eller personlig observation av en person eller ett annat objekt. Personbaserad underrättelseinhämtning utomlands kan också bedrivas så att kommunikationen sker genom datanätets kommunikationstjänster från Finland.

Den personbaserade underrättelseinhämtningen kan åstadkomma sådan detaljerad och djupgående information med en högre skyddsnivå som det är svårt eller omöjligt att åstadkomma med andra former av underrättelse. Med hjälp av personbaserad inhämtning kan också förutsättningar skapas för att effektivare utnyttja andra underrättelseformer.

I spaning i utländska datasystem är det fråga om inhämtning av information som behandlas i utländska datasystem med datatekniska metoder. Den centrala skillnaden mellan spaning i utländska datasystem och datatrafikspaning är verksamhetens territoriella utsträckning. Spaningen i utländska datasystem sker på territoriet till den stat som är föremål för spaningen och i vissa fall på en tredje stats territorium utgående från Finland, medan igen datatrafikspaningen försiggår på finskt territorium.

Flera europeiska stater har lagstiftat om sin underrättelseverksamhet utomlands och om de befogenheter som ska användas i den. Från land till land varierar det med vilken exakthet det har ansetts motiverat att lagstifta om de enskilda befogenheterna. Bland andra Sverige representerar en lagstiftningsmodell med allmänna drag. Den svenska underrättelseverksamhetens befogenhetsreglering begränsas av en bestämmelse enligt vilken underrättelseverksamhet bedrivs genom att information inhämtas, bearbetas och analyseras och i verksamheten används teknisk informationsinhämtning och personlig informationsinhämtning. Som exempel på en mera detaljerad regleringsexakthet kan nämnas Nederländerna, där underrättelselagen innehåller noggranna bestämmelser om varje befogenhet som underrättelsetjänsterna har till sitt förfogande.

Internationellt sett är i synnerhet metoderna för spaning i datasystem föremål för en kraftig utveckling. Underrättelsetjänsterna samlar med hjälp av metoderna för spaning i datasystem i vid bemärkelse in information t.ex. om målstatens aktörer och system samt om dess datanäts sammansättningar och sårbarheter. Målet för spaning i utländska datasystem kan vara förutom att inhämta information också att störa datasystemets funktion eller skada det genom att förändra eller förstöra uppgifterna i det. Sådan verksamhet kan i målstaten tolkas som användning av våld eller som ett intrång i suveräniteten som kan jämställas med en väpnad attack.[60] Det om störning eller skadande av ett datasystems funktion ska tolkas som användning av våld beror både på föremålet och på graden av skada som det orsakats. Om endast en tillfällig olägenhet orsakas (överbelastningsattacker) är det ännu inte användning av våld. Däremot, om föremålet för en operation är betydande, den varar länge och intensiteten är hög, kan operationen tolkas som användning av våld, men inte nödvändigtvis ännu som en väpnad attack.

Den spaning i datasystem som föreslås i detta betänkande ska inte till sin art vara verksamhet av arten användning av våld som kan jämföras med nätattacker, utan det ska vara fråga om att inhämta underrättelseinformation som en del av den övriga underrättelseverksamheten. Utgångspunkten för spaning i datasystem ska vara att samla in information ur ett datasystem så obemärkt som möjligt och syftet är inte t.ex. att störa funktionen i det datasystem som är föremål för verksamheten eller att förändra eller förstöra den information som datasystemet innehåller. Även om de juridiska tolkningar och bedömningar som gäller datanätsoperationer endast håller på att formas och man i den internationella rätten inte har kunnat definiera tröskeln för en attack som görs i en datanätsomgivning, verkar det som om dylik spaning i datasystem, som kan jämställas med inhämtandet av underrättelseinformation, inte kan tolkas som användning av våld som strider mot den internationella rätten och åtminstone inte som en attack.[61] För denna syn talar det att såvitt man känner till har ingen stat vidtagit väpnade försvarsåtgärder mot den stat som har riktat spaning i datasystem mot den. Åtgärder som riktar sig mot datasystem har hittills inte obestridligen och offentligt beskrivits som en väpnad attack i det internationella samfundet.[62]

6.2.2 Utvecklingsbehov

För att Finlands centrala säkerhetsintressen ska kunna skyddas är det nödvändigt att skapa en författningsgrund för den inhämtning av underrättelseinformation utomlands som de civila och militära myndigheter som svarar för den nationella säkerheten utför i utlandet. Syftet med verksamheten bör vara att utgöra ett stöd för den högsta statsledningens utrikes- och säkerhetspolitiska beslutsfattande samt att avvärja allvarliga

[60] Tallinn Manual on the International Law applicable to Cyber Warfare, Cambridge University Press 2013, den s.k. Tallinnmanualen är ett icke-bindande dokument, som internationellt uppskattade experter på internationell rätt har upprättat i egenskap av privatpersoner och som gäller den internationella rätt som ska tillämpas på cyberkrigföring och som trots dess inofficiella karaktär tämligen allmänt används som referensmaterial.
[61] Tallinnmanualen, s. 50 och 52.
[62] Tallinnmanualen, s. 57

yttre säkerhetshot som riktas mot Finland. Dessa är i synnerhet militära hot som riktas mot landet, hot som riktas mot sådana internationella krishanteringsinsatser där Finland är med, internationell terrorism som riktas mot landet, främmande staters underrättelseverksamhet som riktas mot landet, internationell organiserad brottslighet som äventyrar den nationella säkerheten, utvecklande, spridning och export av massförstörelsevapen, försvarsmateriel och produkter med dubbla användningsområden, andra allvarliga hot som riktas mot samhällets vitala funktioner, framför allt näthot, sådana planer, avsikter och åtgärder hos en främmande makt som kan påverka den finska utrikes- och säkerhetspolitiken skadligt eller menligt eller vilka kan vara av betydelse för den finska utrikes- och säkerhetspolitiken.

En författningsgrund behövs både för den personbaserade underrättelseinhämtningen utomlands och för spaningen i utländska datasystem.

Utgående från den internationella jämförelse som gjorts vore det orsak att i det fortsatta arbetet överväga om det vid personbaserad underrättelseinhämtning utomlands skulle vara möjligt att använda personkällor samt inhämta information genom att göra planenliga observationer av personer, platser och andra objekt. Likaså borde det övervägas om informationsinhämtningen kunde skyddas så att den hemlighålls för att informationsinhämtarens eller informationsöverlåtarens säkerhet ska kunna tryggas, för att det förtroende som krävs för informationsinhämtningen ska kunna etableras eller för att röjning av informationsinhämtningen ska kunna förhindras.
Personbaserad underrättelseinhämtning utomlands kunde grunda sig på personligt umgänge mellan den tjänsteman som utövar informationsinhämtningen och en utomstående person. Det bör övervägas om man förutom att be en personkälla överlämna den information hen har också kunde ge hen direktiv om att inhämta information. Identiteten och bakgrundsorganisationen för den tjänsteman som bedriver underrättelseinhämtning ska, när detta är nödvändigt, kunna hemlighållas.
Utöver att personbaserad inhämtning ska göras utomlands, ska sådan också kunna göras via datanätets kommunikationstjänster från Finland. Personbaserad underrättelseinhämtning ska också kunna utföras som en del av en krishanteringsinsats.

Med spaning i utländska datasystem ska avses säkerhetsmyndigheternas aktiva verksamhet för att inhämta information via nätet om sådana enskilda eller statliga aktörer som befinner sig utomlands och vilka kan hota Finlands nationella säkerhet eller andra för samhället vitala intressen. Spaning i datasystem möjliggör att man kan bereda sig på och bemöta hot som riktas mot skyddsstrukturerna och skyddsåtgärderna i Finlands kritiska datasystem. Sist och slutligen blir det, genom den information som spaning i utländska datasystem ger, möjligt att vid datanätskrigföring inrikta påverkan på kapaciteterna på motståndarens objekt som en del av användningen av militära maktmedel i krissituationer.

Spaning i datasystem förutsätter att det tekniska skyddet kan förbigås samt att verksamhet kan bedrivas i datanät utanför den finska riksgränsen.

Det att åtgärder med anknytning till underrättelse utomlands anses oberättigade måste slopas genom att om detta lagstiftas nationellt. I en eventuell kommande lagberedning bör det granskas vilka behov av ändringar det finns t.ex. i den straff- och tjänstemannarättsliga regleringen. Vidare bör i verksamheten beaktas de internationella människorättsfördrag och andra internationella förpliktelser som binder Finland.

6.2.3 Målstatens synvinkel

Enligt en allmän princip i den internationella rätten åtnjuter varje suverän stat territoriell integritet och politisk oavhängighet i relation till övriga stater. Varje stat beslutar själv om den tillåter, och på vilka villkor i så fall, att utländska tjänstemän är verksamma på dess territorium. Ovan har det konstaterats att de flesta stater de facto till en viss gräns tål eller till och med godtar främmande underrättelsemyndigheters verksamhet inom sitt territorium. Det kan vara frågan om ett informationsutbyte som båda parter har nytta av eller att informationsinsamling som en främmande stat gör öppet och som gäller de allmänna förhållandena i målstaten inte äventyrar målstatens eller någon annan parts intressen. Under andra förhållanden kan målstaten förhålla sig negativt till en främmande stats myndigheters verksamhet på dess territorium. Verksamheten kan också från fall till fall uppfylla brottsrekvisitet på någon gärning som i målstatens strafflagstiftning har föreskrivits som straffbar. Huruvida en verksamhet är straffbar eller inte kan, beroende på målstat, påverkas av t.ex. vem det är som inhämtar information, hurdan information som inhämtas och med vilken metod informationsinhämtningen sker.

Jämförelsestaterna har inte på lagstiftningsnivå ställt som villkor för spaning utomlands att målstaten godkänner verksamheten eller att genom den inte ska brytas mot målstatens lagstiftning. När man i Finland överväger att skapa en författningsgrund för underrättelse, är det naturligt att granska saken ur samma synvinkel. Vid spaning utomlands ska det vara frågan om verksamhet som är nödvändig för att ett godtagbart mål (säkerställandet av den nationella säkerheten) ska kunna uppnås, och denna verksamhet kan i vissa situationer innehålla risker. En av riskerna är att det är frågan om verksamhet som strider mot målstatens lagstiftning eller annars är icke-godtagbar verksamhet av detta slag. I spaning utomlands vore det viktigt att observera hur övriga stater förhåller sig samt innehållet i deras lagstiftning, men av praktiska skäl kan observationen inte göras när det lagstiftas om verksamheten, utan först när man skrider till verket i den. Då gäller det att överväga, om den fördel som verksamheten medför för den nationella säkerheten är klart större än de risker som är förknippade med den.

6.2.4 Tredje stats synvinkel

Enligt en allmän princip i den internationella rätten åtnjuter varje suverän stat territoriell integritet och politisk oavhängighet i relation till övriga stater. Detta gäller också när spaning sker genom att en tredje stats territorium används på något sätt.

Vidare får en stat enligt en allmän princip i den internationella rätten inte tillåta att dess territorium används för gärningar som skadar eller olagligen påverkar andra stater. När en gärning bedöms, ges betydelse inte endast åt det, om gärningen orsakar skada på egendom eller personer, utan det kan räcka med att gärningen över huvud taget orsakar negativa verkningar.

I personbaserad underrättelseinhämtning utomlands kan man på en tredje stats territorium träffa personer som ger information eller också kan de värvas i en tredje stat. Principen om transiteringsstat kan dock inte anses lämpa sig direkt på den internationella datakommunikationen, där datakommunikationen normalt rör sig och rutterna för den bestäms på ett sätt som inte har definierats på förhand enligt var datakommunikationen i sitt förlopp inte stöter på hinder.

Informationsinhämtning kan man bli tvungen att genomföra på en tredje stats territorium, via det eller i ett datasystem beläget i en annan stat än de personer som innehar den information som är föremål för informationsinhämtningen. Denna konstellation gäller i lika hög grad personbaserad underrättelseinhämtning som spaning i datasystem, men informationsinhämtningens konsekvenser för det tredje landets suveränitet kan anses vara olika. Till exempel en grupp som planerar ett terrordåd i västländerna kan kommunicera via en kommunikationstjänst, som har hyrts för gruppens räkning i ett tredje land, som inte har någon annan beröringspunkt med gruppens medlemmar än servern. Även om den informationsinhämtning som riktas mot en sådan tjänst tekniskt sker i ett datanät som befinner sig på det tredje landets territorium, inriktas verkningarna av informationsinhämtningen på det land där de personer som bedriver verksamheten befinner sig. Konsekvenserna för suveräniteten gäller således i första hand det land där de agerande personerna befinner sig. För att det ska gå att reda ut i vilket land servern är belägen kan det också krävas att man agerar via ett eller flera tredje länder.

Kränkning av en tredje stats suveränitet bör även övervägas i en sådan situation där en server på ett tredje lands territorium används för att vilseleda mållandet t.ex. för att föra in ett underrättelseprogram i det datasystem som är mål för verksamheten. Av betydelse är huruvida myndigheterna i den tredje staten tillåter verksamheten eller inte.

6.2.5 Underrättelseverksamheten och internationell rätt

Enligt artikel 38 i den internationella domstolens grundstadga är den internationella rättens centralaste källor de internationella konventionerna och specialfördragen, internationell sedvanerätt och de s.k. allmänna rättsprinciperna.

Inga internationella fördrag har upprättats om underrättelseverksamhet i fredstid. De bestämmelser om skydd för spioner under krigstid, vilka ingår i artikel 46 i första tilläggsprotokollet till Genevekonventionen från år 1949, har ingen betydelse med tanke på det tema som behandlas här.

Även om det i underrättelseverksamheten i princip är fråga om kränkning av målstatens suveränitet, är rättslitteraturen inte enig om huruvida den internationella rätten på sedvanerättens och de allmänna rättsprincipernas nivå förhåller sig accepterande eller

fördömande till underrättelseverksamhet.[63] Underrättelseverksamheten torde inte kunna anses ha en internationellt rättsligt allmänt godkänd ställning, eftersom stater genom att konstatera att en person är persona non grata eller på annat sätt inte godtagbar upprepade gånger visar att de inte godkänner dylik verksamhet. Å andra sidan kan underrättelseverksamhet inte heller anses vara internationellt rättsligt förbjuden, eftersom nästan alla stater bedriver sådan verksamhet. Det är frågan om en globalt etablerad verksamhet, till vilken de enskilda staternas förhållningssätt bestäms av om de i fallet i fråga innehar rollen som den stat som bedriver underrättelse eller som målstat. Även om underrättelseverksamheten inte är reglerad, visar flera internationella exempel att de möjligheter som det internationella fördragssystemet ger har utnyttjats i verksamheten. I den har använts den immunitet och befrielse från målstatens juridiska domsaga som garanteras en diplomatisk representant i Wienkonventionen om diplomatiska förbindelser (FördrS 3–5/1970).

6.2.6 Beslutsfattandet om underrättelse utomlands

I den internationella jämförelsen kan man upptäcka att beslutsfattandet gällande informationsinhämtning varierar från land till land. För beslutsfattandet kan t.ex. underrättelsemyndigheten själv eller en politiskt ansvarig part svara. Om det är underrättelsemyndigheten som svarar för beslutsfattandet, gör den det inom ramen för de riktlinjer som statsledningen har dragit upp.

Eftersom med underrättelse utomlands sammanhänger utrikespolitiskt sensitiva element, kunde beslutsfattandet i Finland ske under den utrikes- och säkerhetspolitiska ledningens styrning. I Finland behandlar det gemensamma mötet mellan det utrikes- och säkerhetspolitiska ministerutskottet och republikens president i förberedande grad viktiga ärenden som gäller utrikes- och säkerhetspolitiken och andra ärenden som gäller Finlands relation till främmande stater, viktiga ärenden inom den inre säkerheten med anknytning till dessa samt viktiga ärenden som gäller totalförsvaret. De metoder som används i underrättelse riktas mot en främmande stats suveränitet förutom i mållandet också när man samarbetar med en tredje stat eller via en tredje stat till mållandet. Till följd av detta framhävs den politiska dimensionen vid underrättelse utomlands. Underrättelsens eventuella verkningar och risker påverkar beslutsförfarandet. När beslutsförfarandet i fråga om underrättelse utomlands övervägs i det fortsatta arbetet är det viktigt att säkerställa att beslutsförfarandet också fungerar och att den information som är förknippad med det förmedlas i en brådskande situation.

6.2.7 Övervakning

Förutom att om underrättelseverksamhet utomlands ska föreskrivas i lag och denna verksamhet ska utföras under tjänsteansvar, bör verksamheten övervakas såväl juridiskt som också parlamentariskt.

Den juridiska övervakningen ska koncentrera sig på att Finlands lag följs i underrättelseverksamheten utomlands. Utomstående juridisk övervakning ska åtminstone justiti-

[63] Se de översikter som gäller internationell rättslitteratur t.ex. i följande källor: Baker, Christopher D: Tolerance of International Espionage: A Functional Approach (American University International Law Review vol 19 (2003) issue 5); Radsan, Afsheen John: The Unresolved Equation of Espionage and International Law (Michigan Journal of International Law vol 28 (2007) issue 597).

ekanslern och riksdagens justitieombudsman samt dataombudsmannen utföra i enlighet med sina lagstadgade uppgifter. Utöver detta kan det övervägas om det behövs ett utomstående specialövervakningsorgan. Samtidigt bör det sörjas för organisationernas interna laglighetsövervakning samt sådan övervakning som de styrande ministerierna utför.

Till följd av verksamhetens art bör underrättelse utomlands vara underställd parlamentarisk övervakning. I den internationella jämförelsen kan man upptäcka att i vissa länder utförs den parlamentariska övervakningen av ett utskott i riksdagen, medan igen i andra länder för övervakningen svarar ett organ utanför parlamentet, där det finns såväl parlamentarisk som juridisk representation.

6.2.8 Ekonomiska konsekvenser och personalkonsekvenser

På hur stora de ekonomiska konsekvenserna blir inverkar verksamhetens omfattning och hur den inriktas. I princip ska verksamheten bedrivas inom ramen för myndigheternas anslagsramar. Verksamheten ska utvecklas stegvis.

7 SLUTSATSER

Syftet med såväl datatrafikspaning som underrättelse utomlands ska vara att inhämta underrättelseinformation om allvarliga internationella hot, vilken är nödvändig med tanke på den nationella säkerheten. Med verksamheten ska statens högsta lednings beslutsfattande stödas och tillförsäkras att den grundar sig på korrekt, tidsenlig och tillförlitlig information. Med verksamheten ska det också göras möjligt för behöriga myndigheter att avvärja hoten. Om verksamheten ska föreskrivas i lag.

Underrättelsen ska övervakas både juridiskt och parlamentariskt. Det vore befogat att ordna övervakningen av de olika underrättelsemetoderna så enhetligt som möjligt.

7.1 Datatrafikspaning

Finland bör överväga att utveckla befogenheter för spaning som riktas mot gränsöverskridande datakommunikation för att man ska kunna bemöta den förändring i den yttre säkerhetspolitiska omgivningen som beskrivs i betänkandet.

Datatrafikspaningen ska begränsas till att gälla inhämtning av information om hot som äventyrar den nationella säkerheten. Hoten är till sin art antingen militära eller civila och de kan realiseras antingen i den reella världen eller via datanäten.

Omständigheter som är förknippade med harmoniserade förfaringssätt och med laglighetsövervakningen talar för att det tekniska utförandet av datatrafikspaning bör koncentreras till en myndighet. För en koncentrering talar också ekonomiska skäl. Försvarsmaktens underrättelsetjänst har i dagens läge både den tekniska beredskap som verksamheten förutsätter och de internationella samarbetsrelationer som behövs. Uppdragsgivare kan vara de myndigheter som svarar för avvärjandet av hot samt via dem de parter som svarar för det finska utrikes-, säkerhets- och försvarspolitiska beslutsfattandet. I ett dylikt eventuellt arrangemang bör det föreskrivas i lag om de upp-

gifter som bistår civila myndigheter vid enheten som hör till försvarsmakten samt om civila myndigheters befogenhet att ge enheten uppdrag.

Arbetsgruppen utgår ifrån att det inte ska föreslås några skyldigheter för företagsaktörer att ge krypteringsnycklar eller installera bakdörrar i programvaror och apparater. Emellertid förutsätter organiserandet av verksamheten att teleföretag eller ägare till gränsöverskridande datakommunikationstrådar åläggs att anvisa accesspunkter samt ge de uppgifter detta kräver till den myndighet som svarar för realiserandet av datatrafikspaningen.

De grundläggande fri- och rättigheterna och de mänskliga rättigheterna bör beaktas på korrekt sätt när beredningen av en lagstiftning om datatrafikspaning övervägs. I synnerhet måste det i grundlagen för varje individ tryggade skyddet i fråga om hemligheten för ett förtroligt meddelande beaktas och därmed det att man enligt grundlagen genom lag kan föreskriva om de mest nödvändiga begränsningarna av hemligheten för ett sådant meddelande endast vid undersökning, rättegång och säkerhetskontroll av brott som äventyrar en individs eller samhällets säkerhet eller hemfriden samt under den tid som frihetsberövande varar. Därmed verkar det inte vara möjligt att lagstifta om datatrafikspaning som ska realiseras i underrättelsesyfte utan att ändra grundlagen, möjligen med undantag av sådan spaning som enbart riktar in sig på en främmande stats datatrafik. I det fortsatta arbetet kan man fundera över om det vore möjligt att genomföra effektiv datatrafikspaning i en första fas mera begränsat t.ex. genom att spaningen inriktas på identifikationsuppgifter.

Tillståndsförfarandet och realiseringssättet för datatrafikspaning ska beskrivas tillräckligt exakt. Datatrafikspaningen ska vara föremål för en klar styrning samt en täckande juridisk och parlamentarisk övervakning.

När man bedömer konsekvenserna av datatrafikspaningen bör det beaktas också vilka konsekvenser den har på samhällets digitalisering och företagens verksamhetsbetingelser. I den kommande beredningen måste utöver säkerhetspolitiska aspekter också beaktas näringspolitiska faktorer och sådana faktorer som påverkar utvecklingen av ett digitalt ekosystem. Med tanke på den ekonomiska tillväxten är det nödvändigt att utnyttja de möjligheter som data- och kommunikationsteknologin erbjuder vad gäller att förändra verksamhetssätten och förbättra produktiviteten. I det fortsatta arbetet ska det också i en tillräckligt täckande grad övervägas vilka olika tekniska realiseringssätt det finns i fråga om datatrafikspaning och deras ekonomiska konsekvenser.

7.2 Personbaserad underrättelseinhämtning utomlands och spaning i utländska datasystem

Det bör övervägas att de militära och civila myndigheter som svarar för den nationella säkerheten ska ha en möjlighet att inhämta underrättelseinformation som stöder statens högsta lednings beslutsfattande och gäller yttre säkerhetshot. Det är fråga om att inhämta behövlig information av personer utomlands och från utländska datasystem.

De internationella förpliktelser som binder Finland samt lagstiftningen i den stat från vilken syftet är att inhämta informationen bör beaktas när användningen av underrättelsebefogenheter övervägs och de risker som ingår i detta bedöms.

Till följd av verksamhetens art bör den högsta statsledningens riktlinjer beaktas särskilt i det beslutsfattande som gäller underrättelse utomlands. Underrättelse utomlands är framför allt utrikespolitiskt sensitivt. Verksamhetens styr- och ansvarsförhållanden bör övervägas i samband med den eventuella fortsatta beredningen. Underrättelse utomlands ska övervakas både juridiskt och parlamentariskt.

7.3 Förslag till fortsatta åtgärder

För att en författningsgrund gällande underrättelse ska kunna skapas föreslås det att ett eller flera lagstiftningsprojekt ska inledas på de grunder som beskrivs ovan. Beredningen ska vid behov också kunna genomföras etappvis, men då måste de begränsningar för regleringen av datatrafikspaning som för närvarande följer av grundlagen beaktas. Det bör också övervägas om beredningen kunde vara t.ex. parlamentarisk eller annars ske under politisk styrning.

Eftersom behoven inom inrikesministeriets förvaltningsområde sammanhänger med upptäckandet av allvarliga hot av civil art, såsom terrorism och spioneri, vilka äventyrar den internationella säkerheten och med identifieringen av de aktörer som ligger bakom dessa hot, kunde det övervägas att den lagstiftning som sammanhänger med civil underrättelse skulle beredas under inrikesministeriets ledning.

Behoven inom försvarsministeriets förvaltningsområde gäller för sin del bildandet och upprätthållandet av en lägesbild, givandet av en förvarning samt stöd till målanvisning, vilka anknyter till försvarsmaktens uppgifter. Därför kunde beredningen av den lagstiftning som gäller militär underrättelse göras under försvarsministeriets ledning.

Eftersom datatrafikspaning vore nödvändig på båda förvaltningsområdena, bör det övervägas om en särskild lag om datatrafikspaning ska stiftas. I denna beredning bör också intressegruppernas behov uppmärksammas och sörjas för att företrädare för näringslivet finns med.
En eventuell justering av grundlagen bereds under justitieministeriets ledning.
Om underrättelselagstiftningen bereds sektorvis inom förvaltningsområdena, bör det sörjas för att beredningen samordnas.

Bilaga 1

gearshiftgroup

Utvecklingen i fråga om utländska investeringar inom IT-sektorn i Sverige och Finland åren 2008 – 2013 och den svenska FRA-lagens eventuella konsekvenser för investeringarna

INNEHÅLL

1 Det temaområde som ska granskas

1.1 Bakgrund och mål

Försvarsministeriet har tillsatt en arbetsgrupp som har i uppdrag att utveckla den finska lagstiftningen särskilt vad gäller regleringen av säkerhetsmyndigheternas informationsinhämtning. Målet är att det ska sörjas bättre för den nationella säkerheten för att hot i datanäten ska kunna avvärjas.
I denna utredning bedöms denna sak med tanke på utvecklingen av de utländska investeringarna inom IT-sektorn i Sverige och Finland under 2008 – 2013. Som slutresultat av utredningen görs ett sammandrag av utvecklingen samt en bedömning av ”FRA-lagens” eventuella konsekvenser för de realiserade investeringarna i Sverige.
Bestämmelser om signalspaning finns i speciallagar och en specialförordning om detta: Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet, Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet och Förordning (2008:923) om signalspaning i försvarsunderrättelseverksamhet. Signalspaning utförs av försvarsmaktens radioanstalt (FRA), som är en civil organisation underställd försvarsdepartementet. FRA har till uppgift att inhämta underrättelseinformation i enlighet med de uppdrag anstalten fått och ställa informationen till uppdragsgivarnas förfogande.

1.2 Avgränsning av utredningen

I denna utredning koncentrerar man sig på hur de utländska investeringarna på IT-sektorn har utvecklat sig i Sverige och Finland åren 2008–2013 samt bedömer vilka eventuella konsekvenser Sveriges ”FRA-lag” har på investeringarna ur följande granskningssynvinklar:

- konsekvenser för investeringarna och förutsättningarna för dem
- konsekvenser för FoU verksamheten i Sverige
- konsekvenser för Sveriges internationella konkurrenskraft
- konsekvenser för uppkomsten av ny företagsverksamhet i Sverige och Finland
- konsekvenser för olika företag eller företagsgrupper i Sverige

1.3 De metoder som använts

Som metod har använts en litteraturstudie av de ekonomiska verkningarna av ”Internet Surveillance” -lagstiftningen. Utöver konsekvenserna av lagstiftningen har man försökt hitta studier på temat hur bevakningen har påverkat investeringarna. Förutom egentliga forskningskällor har man samlat in information från marknadsundersökningsinstitutens rapporter samt sakkunnigutvärderingar som kan hittas via medierapporter. Utgående från litteraturstudien har det bedömts på vilka saker lagstiftningen och verkningen av den har konsekvenser samt hur stor verkan det är frågan om. På basis av litteraturstudien samt statistisk sektorinformation och annan dylik information bedöms verkningens storlek i Sverige samt jämförs den med den verkliga utvecklingen under åren 2008 – 2013 jämfört med Finland.

2 Nyhetsförmedlingen i Sverige och Finland innan lagen trädde i kraft

2.1 Google Sverige

”Google likens Sweden to dictatorship”, Published: 30 May 2007 11:49 GMT+02:00
“Search engine giant Google has slammed Sweden’s proposed wiretapping legislation as illiberal and incompatible with Western democracy”. Speaking on a visit to Sweden on Tuesday, the company’s global privacy counsel, Peter Fleischer, warned that Google would rule out making any major investments in Sweden should the controversial bill become law.
“We have contacted Swedish authorities to give our view of the proposal and we have made it clear that we will never place any servers inside Sweden’s borders if the proposal goes through.” Fleischer told Internet World.

2.2 Aftonbladet Sverige

2008-06-19, IT-företag undviker Sverige efter FRA-lag. ”Flera stora företag vill inte satsa här” Sverige går miste om stora investeringar från multinationella IT-företag. FRA-lagen gör att de inte vill lägga sin verksamhet här enligt myndigheten Invest in Sweden Agency. ”Vi har fått tydliga besked från flera stora företag att de inte vill satsa här”, säger Bengt-Åke Ljudén, försäljningschef på Invest in Sweden Agency (ISA), en statlig myndighet som hjälper utländska företag till Sverige. ”Sverige lämpar sig annars särskilt väl för internetoperatörer som kräver tillgång till energi och kyla för sina servrar”, enligt Ljudén. ”Vi får väldigt många förfrågningar från företag som vill bygga upp stora datacenter”.

IT-företaget Intel har nyligen investerat stora pengar i Sverige i utbyggnaden av fjärde generationens mobiltelefoni. Tvärtemot Invest in Sweden Agency tror Carl-Daniel Norenberg, affärsutvecklare på Intel, inte att FRA-lagen har betydelse för investeringsviljan. ”Det här påverkar inte på något sätt vår verksamhet. Vi rullar på som vanligt”, säger han till TT.

2.3 Den finska diskussionen

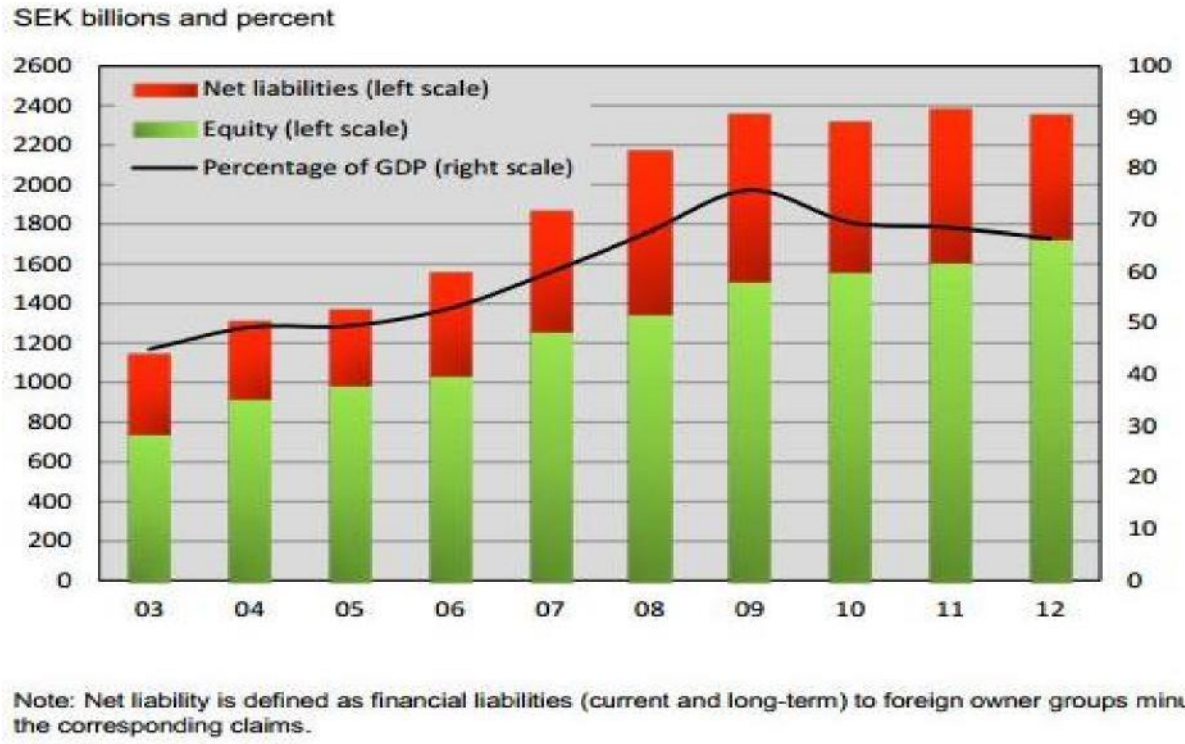
Teknologiindustrier sparkade kraftigt bakut i fråga om den föreslagna ”masssnokarlagen”.
10.3.2014 13:00, It-viikko

”Representanterna för Finlands regering bygger luftslott på datakabelspel och Finlands möjlighet att stiga fram som Europas ”dataäss” eller bli ett ”dataSchweiz”. Men samtidigt håller man inom regeringen på och bygger ihop en lag om informationsinsamling som kritikerna kallar en ”massnokarlag”. Teknologiindustrier rf är rädd för att lagprojektet i sin strävan att förbättra polisens verksamhetsbetingelser i den digitala världen förstör Finlands rykte som ett dataskyddat och neutralt land och tar kål på den spirande databusinessen i dess linda.

3. Granskningens synvinklar

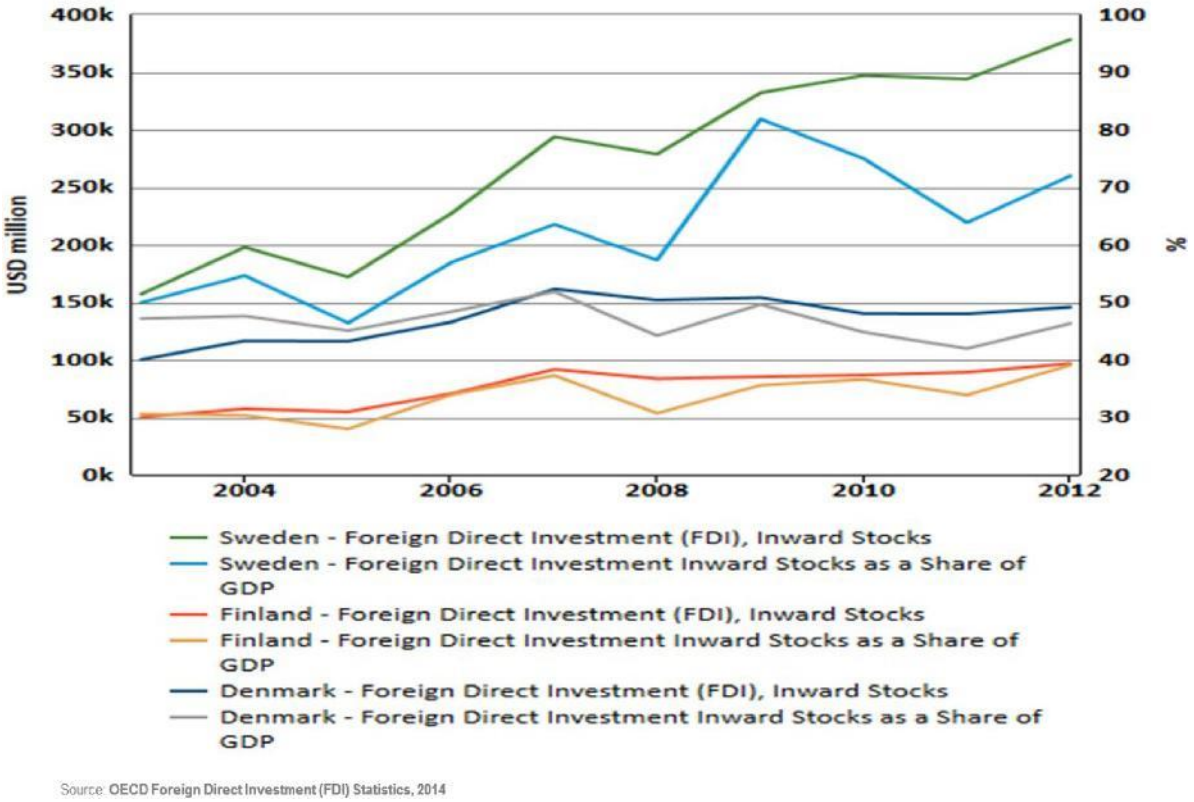
3.1 Konsekvenser för investeringarna och förutsättningar för dem

I figur 1, som beskriver den allmänna utvecklingen av utländska investeringar i Sverige, finns ingen sådan avvikelse i investeringsutvecklingen efter att lagen trädde i kraft år 2009 som man kunde motivera med verkan från FRA-lagen. Det att den uppåtgående utvecklingen bröts år 2009 kan förklaras med bankkrisen, som skakade hela världen, och det allmänna sammanbrottet i investeringstillväxten som var en följd av krisen. Figuren skildrar inte i sig ändringarna i mängden investeringar i IT-sektorn, men de anses följa samma slags utveckling utgående från kommentarerna från experter i sektorn.



Figur 1. Utvecklingen av utländska investeringar i Sverige.

En mera vidsträckt bild av den svenska FRA-lagens konsekvenser för hela området av utländska investeringar får man om man jämför utvecklingen i Sverige, Finland och Danmark. I figur 2 kan man se att det att lagen trädde i kraft inte hade någon klar betydelse för utvecklingen i fråga om de utländska investeringarna i Sverige jämfört med i Finland och Danmark. Inte heller i denna figur har investeringarna i IT-sektorn specificerats, men de har följt den allmänna utvecklingen i alla länder som är med i jämförelsen.



Figur *2. De utländska investeringarnas storlek i miljoner dollar och andelen av BNP i Sverige, Finland och Danmark.*

Utifrån de föregående figurerna kan man på en allmän nivå konstatera att det inte finns något klart samband mellan orsak och verkan i utvecklingen i fråga om mängden utländska investeringar vad gäller FRA-lagens ikraftträdande år 2009.

3.2 Konsekvenser för FoU-verksamheten i Sverige

När andelen forsknings- och utvecklingsutgifter i tabell 1 granskas i förhållande till BNP i Sverige och Finland är det svårt att se någon betydande avvikelse i utvecklingstrenden. De svenska forsknings- och utvecklingsutgifterna i förhållande till BNP sjönk något från år 2009 framåt, i Finland började nedgången år 2011. Det bör emellertid observeras att även efter att nivån sjunkit är Sverige och Finland i topp vad gäller utvecklingsutgifternas andel av BNP och på en klart högre nivå än övriga länder i jämförelsegruppen i EU. Det är svårt att se att den sjunkande trenden gällande utvecklingsutgifter skulle ha något samband med FRA-lagen, under samma period infaller också den globala ekonomiska recessionen och en strängare budgethantering hos de ekonomiska aktörerna, och den nedåtgående utvecklingen kan också ses i de finska siffrorna med en liten fördröjning.

Tabell 1. Forsknings- och utvecklingsutgifternas andel av BNP 2002 – 2010.

	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
EU-28	*1.87*	1.86	1.82	1.82	1.84	1.84	*1.91*	*2.01*	*2.00*	*2.04*	*2.06*
Euro area (EA-17)	*1.88*	1.87	1.85	1.84	1.87	1.88	*1.96*	*2.06*	*2.07*	*2.12*	*2.14*
Belgium	1.94	1.87	1.86	1.83	1.86	1.89	1.97	2.03	2.10	2.21	*2.24*
Bulgaria	0.48	0.48	0.49	0.46	0.46	0.45	0.47	0.53	0.60	0.57	*0.64*
Czech Republic	1.15	1.20	1.20	1.22	1.29	1.37	1.30	1.35	1.40	1.64	*1.88*
Denmark (1)	2.51	2.58	2.48	2.46	2.48	2.58	2.85	3.16	3.00	2.98	*2.99*
Germany	2.50	2.54	2.50	2.51	2.54	2.53	2.69	2.82	2.80	2.89	*2.92*
Estonia	0.72	0.77	0.85	0.93	1.13	1.08	1.28	1.41	1.62	2.37	*2.18*
Ireland	1.10	1.16	1.23	1.25	1.25	1.28	1.45	1.69	*1.69*	*1.66*	*1.72*
Greece (2)	:	0.57	*0.55*	0.60	*0.59*	*0.60*	:	:	:	0.67	0.69
Spain	0.99	1.05	1.06	1.12	1.20	1.27	1.35	1.39	1.40	1.36	1.30
France (3)	2.24	2.18	2.16	2.11	2.11	2.08	2.12	2.27	2.24	2.25	*2.26*
Croatia	0.96	0.96	1.05	0.87	0.75	0.80	0.90	0.85	0.75	0.76	0.75
Italy	1.12	1.10	1.09	1.09	1.13	1.17	1.21	1.26	1.26	1.25	*1.27*
Cyprus	0.30	0.35	0.37	0.41	0.43	0.44	0.43	0.49	0.50	0.50	*0.47*
Latvia	0.42	0.38	0.42	0.56	0.70	0.60	0.62	0.46	0.60	0.70	*0.66*
Lithuania	0.66	0.67	0.75	0.75	0.79	0.81	0.80	0.84	0.79	0.91	*0.90*
Luxembourg	:	1.65	1.63	1.56	1.66	*1.58*	1.66	1.74	1.51	:	:
Hungary (4)(5)	1.00	0.94	0.88	0.94	1.01	0.98	1.00	1.17	1.17	1.22	1.30
Malta (4)	0.25	0.25	0.51	0.55	0.60	0.57	0.55	0.53	0.66	0.72	*0.84*
Netherlands (3)	1.88	1.92	1.93	1.90	1.88	1.81	1.77	1.82	1.86	2.03	*2.16*
Austria	2.12	*2.24*	2.24	*2.46*	2.44	2.51	*2.67*	2.71	*2.80*	2.77	*2.84*
Poland	0.56	0.54	0.56	0.57	0.56	0.57	0.60	0.67	0.74	0.76	0.90
Portugal (6)	*0.73*	0.71	*0.74*	0.78	*0.99*	1.17	1.50	1.64	1.59	1.52	*1.50*
Romania (2)(7)	0.38	0.39	0.39	0.41	0.45	0.52	0.58	0.47	0.46	0.50	*0.42*
Slovenia (3)(8)	1.47	1.27	1.39	1.44	1.56	1.45	1.66	1.85	2.10	2.47	*2.80*
Slovakia	0.57	0.57	0.51	0.51	0.49	0.46	0.47	0.48	0.63	0.68	0.82
Finland	3.36	3.44	3.45	3.48	3.48	3.47	3.70	3.94	3.90	3.80	3.55
Sweden (4)	:	3.80	3.58	3.56	*3.68*	3.43	*3.70*	3.62	*3.39*	3.39	*3.41*
United Kingdom	1.78	1.73	1.67	1.70	1.72	1.75	*1.75*	*1.82*	*1.77*	1.78	*1.72*
Iceland	*2.95*	2.82	:	2.77	2.99	2.68	2.65	3.11	:	2.40	:
Norway	1.66	1.71	1.57	1.51	1.48	1.59	1.58	1.76	1.68	1.65	1.66
Switzerland	:	:	2.82	:	:	:	2.87	:	:	:	:
Serbia	:	:	:	:	:	:	:	0.92	0.79	0.77	0.96
Turkey	0.53	0.48	0.52	0.59	0.58	0.72	0.73	0.85	0.84	0.86	:
China (except Hong Kong)	1.07	1.13	1.23	1.32	1.39	1.40	1.47	1.70	1.76	1.84	:
Japan (4)	3.12	3.14	3.13	3.31	3.41	3.46	3.47	3.36	3.25	:	:
United States (4)	2.52	2.52	2.45	2.49	2.55	2.62	2.76	2.81	2.73	2.67	:

(1) 2007: break in series. 2009: definition differs.
(2) 2011: break in series.
(3) 2004 and 2010: break in series.
(4) 2004: break in series.
(5) 2002 and 2003: definition differs.
(6) 2008: break in series.
(7) 2012: definition differs.
(8) 2005: break in series. 2003, 2004, 2006 and 2010: definition differs.
(9) 2006: break in series. Definition differs.
Note: when definitions differ, see http://epp.eurostat.ec.europa.eu/cache/ITY_SDDS/EN/rd_esms.htm.
Source: Eurostat (online data codes: t2020_20 and rd_e_gerdtot), OECD

Som en andra granskningssynvinkel kan man använda utvecklingen i fråga om källfinansiering vad gäller satsningarna på forsknings- och utvecklingsutgifter. Tabell 2 beskriver fördelningen av finansieringskällor för att täcka forsknings- och utvecklingsutgifterna åren 2007 och 2011. I utvecklingen i fråga om finanskällor i Sverige kan man upptäcka att de utländska parterna till och med klart har ökat sina satsningar under jämförelseperioden i relation till de satsningar som kommer inifrån Sverige både från den privata och den offentliga sektorn. Detta ger starka indicier på att FRA-lagen inte har haft någon betydelse för inriktningen av utländska forsknings- och utvecklingssatsningar. Det att nivån på utvecklingsutgifterna i Sverige har sjunkit förklaras till en stor del med att de svenska bolagen och den offentliga sidan har slagit på bromsarna.

Tabell 2. Forsknings- och utvecklingsutgifternas finansieringskällor 2007 och 2011.

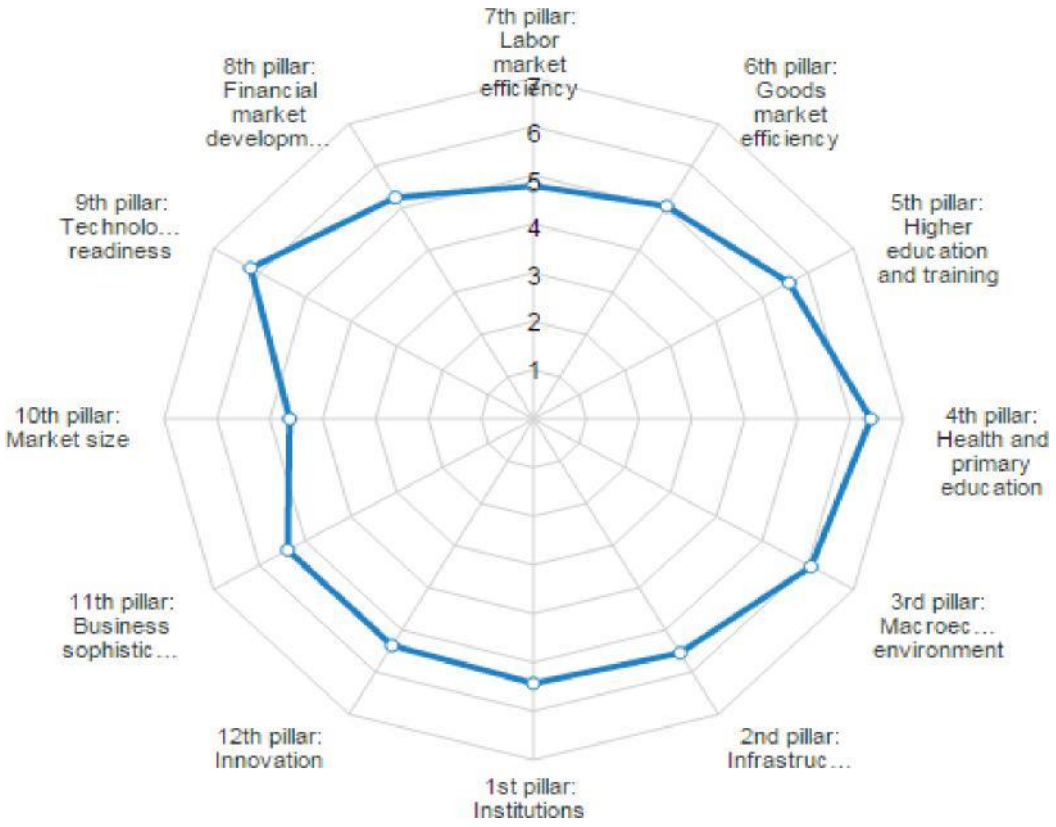
	Business enterprise sector		Government sector		Abroad	
	2007	2011	2007	2011	2007	2011
EU-28	*54.9*	*54.9*	*33.3*	*33.4*	*9.2*	*9.2*
Euro area (EA-17)	*56.7*	*56.8*	*34.0*	*33.9*	*7.4*	*7.4*
Belgium	61.4	60.2	22.2	23.4	13.0	13.0
Bulgaria	34.2	16.9	56.7	38.8	7.6	43.9
Czech Republic	47.2	37.7	44.7	41.7	7.3	19.7
Denmark (1)	61.0	60.3	25.9	28.9	9.5	7.2
Germany	68.1	65.6	27.5	29.8	4.0	4.2
Estonia	41.6	55.0	45.6	32.8	11.7	11.9
Ireland	49.5	*48.4*	32.4	*30.3*	15.8	*20.1*
Greece	:	32.7	:	49.2	:	14.8
Spain	45.5	44.3	43.7	44.5	7.0	6.7
France (2)	52.3	55.0	38.1	35.4	7.5	7.7
Croatia	35.5	38.2	50.4	48.2	10.9	11.6
Italy	42.0	45.1	44.3	41.9	9.5	9.1
Cyprus	16.4	11.0	64.6	70.6	14.5	14.1
Latvia	36.4	24.8	49.9	22.5	12.7	51.0
Lithuania	32.8	28.2	46.9	42.2	19.6	28.4
Luxembourg (3)	76.0	44.3	18.2	34.8	5.7	20.7
Hungary	43.9	47.5	44.4	38.1	11.1	13.5
Malta	51.9	51.9	25.7	29.0	22.4	16.8
Netherlands (2)	48.8	49.9	38.0	35.5	10.7	10.9
Austria	48.7	46.2	32.3	35.8	17.9	16.9
Poland	34.3	28.1	58.6	55.8	6.7	13.4
Portugal (2)	47.0	44.0	44.6	41.8	5.4	5.9
Romania (2)	26.9	37.4	67.1	49.1	4.5	12.1
Slovenia (2)	58.3	61.2	35.6	31.5	5.8	7.0
Slovakia (4)	35.6	33.9	53.9	49.8	10.2	14.2
Finland (5)	68.2	67.0	24.1	25.0	6.5	6.5
Sweden	62.8	57.3	24.6	27.7	9.6	11.1
United Kingdom	46.0	45.9	30.9	30.5	17.3	17.8
Iceland	50.4	47.5	38.8	42.3	10.0	8.4
Norway	45.0	44.2	44.9	46.5	8.5	7.8
Switzerland (6)	68.2	:	22.8	:	6.0	:
Serbia (7)	8.3	9.1	62.9	63.4	7.2	5.5
Turkey (8)	48.4	45.8	47.1	29.2	0.5	0.7
China (except Hong Kong) (8)	70.4	73.9	24.6	21.7	1.3	1.3
Japan (2)(3)(4)	77.7	75.9	15.6	17.2	0.3	0.4
United States (8)	64.9	*60.0*	29.1	33.4	:	:

(1) Government sector, 2007: definition differs.
(2) Break in series.
(3) 2010 instead of 2011.
(4) Government sector: definition differs.
(5) Government sector: break in series.
(6) 2008 instead of 2007.
(7) 2009 instead of 2007.
(8) Business enterprise and government sectors: break in series. Business enterprise and government sectors, 2007: definition differs.
(8) Definition differs.
Note: when definitions differ, see http://epp.eurostat.ec.europa.eu/cache/ITY_SDDS/EN/rd_esms.htm.
Source: Eurostat (online data code: tsc00031), OECD

Som ett sammandrag av forsknings- och utvecklingsutgifterna kan det konstateras att FRA-lagen inte har haft någon praktisk betydelse på aktiviteten på detta område. Den största faktorn som förklarar förändringarna har varit den ekonomiska utvecklingen och Sveriges starka satsning på forskning och utveckling i relation till BNP, vilken har fortgått trots förändringarna i omgivningen.

3.3 Konsekvenser för Sveriges internationella konkurrenskraft

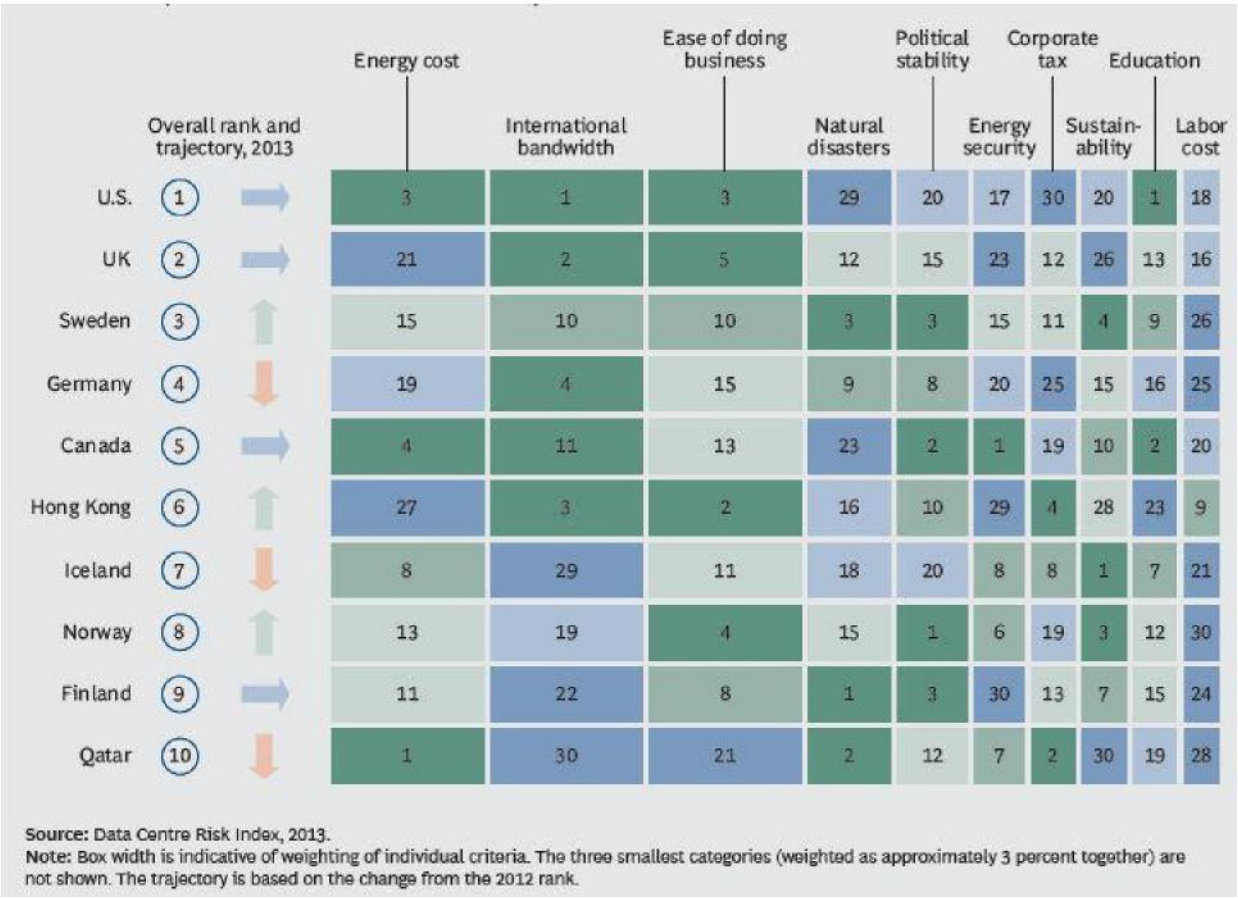
I World Economic Forums jämförelser placerar sig Sverige bland topp tio när man bedömer både den internationella konkurrenskraften och innovationerna. I figur 3 beskrivs Sveriges konkurrenskraft bedömd sektorvis. I figuren kan man se att landet får synnerligen höga bedömningar på flera sektorer. Utifrån dessa konkurrenskraftsfaktorer är det svårt att konstatera vilken direkt betydelse FRA-lagen har på den svenska konkurrenskraften på en allmän nivå, men å andra sidan får infrastrukturen och myndighetsverksamheten höga betyg i denna granskning.



Figur 3. Bedömning av den svenska konkurrenskraften sektorvis. (www.weforum.org).

Betydligt klarare kan olika länders konkurrenskraft med tanke på IT-investeringar bedömas med utgångspunkt i förutsättningarna för datacenterverksamhet. FRA-lagen är starkt kopplad till datacentrens verksamhetsbetingelser och en bedömning av centrens placeringsplats. I tabell 3 finns en internationell riskjämförelse över de viktigaste målländerna för datacentrens placeringsplatser. Denna jämförelse görs årligen. I jämförelsen år 2013 klarar sig Sverige utmärkt och placerar sig på tredje plats. Sverige har klart klättrat i placeringarna från åttonde plats år 2012 till tredje plats, medan Finland placerar sig på nionde plats båda åren. Således kan polemiken vid FRA-lagens uppkomst inte ses i den riskjämförelse som analyserar placeringsplatser. I praktiken kan Sveriges konkurrenskraft på detta område ses i betydande nya datacenterprojekt, bl.a. Facebook 2011 och kapacitetsutbyggnad 2014, KnC Miner 2014, Hydro66 2014 samt Bahnhofs stora utbyggnadsprojekt i Stockholm. I Finland har bl.a. Google, som har genomfört flera utbyggnader, Telecity och Yandex investerat under motsvarande period.

Tabell 3. Riskjämförelse av länderna gällande placeringsplats för datacenter.



	Overall rank and trajectory, 2013	Energy cost	International bandwidth	Ease of doing business	Natural disasters	Political stability	Energy security	Corporate tax	Sustain-ability	Education	Labor cost
U.S.	1 →	3	1	3	29	20	17	30	20	1	18
UK	2 →	21	2	5	12	15	23	12	26	13	16
Sweden	3 ↑	15	10	10	3	3	15	11	4	9	26
Germany	4 ↓	19	4	15	9	8	20	25	15	16	25
Canada	5 →	4	11	13	23	2	1	19	10	2	20
Hong Kong	6 ↑	27	3	2	16	10	29	4	28	23	9
Iceland	7 ↓	8	29	11	18	20	8	8	1	7	21
Norway	8 ↑	13	19	4	15	1	6	19	3	12	30
Finland	9 →	11	22	8	1	3	30	13	7	15	24
Qatar	10 ↓	1	30	21	2	12	7	2	30	19	28

Source: Data Centre Risk Index, 2013.
Note: Box width is indicative of weighting of individual criteria. The three smallest categories (weighted as approximately 3 percent together) are not shown. The trajectory is based on the change from the 2012 rank.

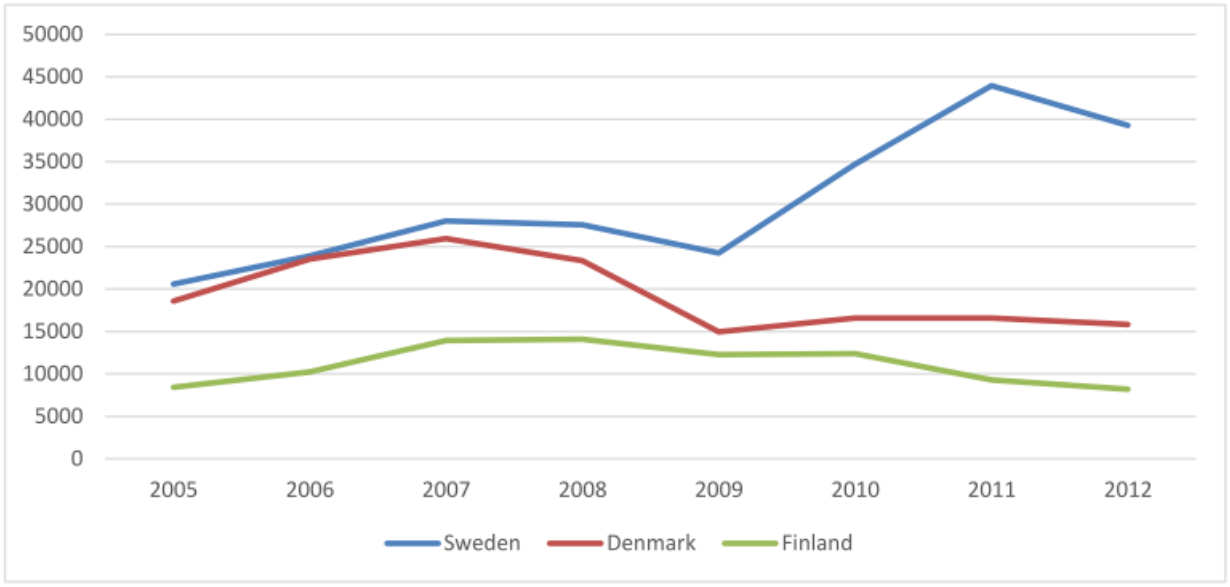
När FRA-lagens konsekvenser för den svenska internationella konkurrenskraften bedöms, verkar den inte ha några negativa konsekvenser, åtminstone inte med tanke på placeringen av datacenter. Datacentren och deras kundkrets täcker olika intressegrupper mycket vidsträckt, vilket gör att synen till denna del är täckande. Inte heller i denna jämförelse av placeringsplatser, som datacentren gör årligen, har lagen i fråga dykt upp.

Å andra sidan verkar det till och med, till följd av den ökande medvetenhet som Snowden-avslöjandena har medfört, som om Sveriges klara spelregler gällande myndigheternas informations-inhämtning är en konkurrensfördel i sin nuvarande form. I fråga om stora långvariga investeringar är en minimering av riskerna och förutsebarheten i utvecklingen av omgivningen betydande faktorer som inverkar på ländernas konkurrenskraft.

3.4 Konsekvenser för uppkomsten av ny företagsverksamhet i Sverige och Finland

Sveriges ICT-sektor har utvecklat sig positivt i relation till den övriga ekonomin under de senaste åren, och tack vare detta har också nya företag och den samhälleliga betydelsen av sektorn ökat med god fart. När man jämför utvecklingen i fråga om grundandet av nya företag i Sverige, Finland och Danmark åren 2005 – 2012 (figur 4), tar Sverige en ovillkorlig topplacering i jämförelsen. FRA-lagen har en mycket liten betydelse i företagens allmänna omgivning, och lagen kan inte anses ha

påverkat utvecklingen av företagsverksamheten eller uppkomsten av nya företag i den ena eller andra riktningen.



Figur 4. Grundade företag 2005 – 2012.

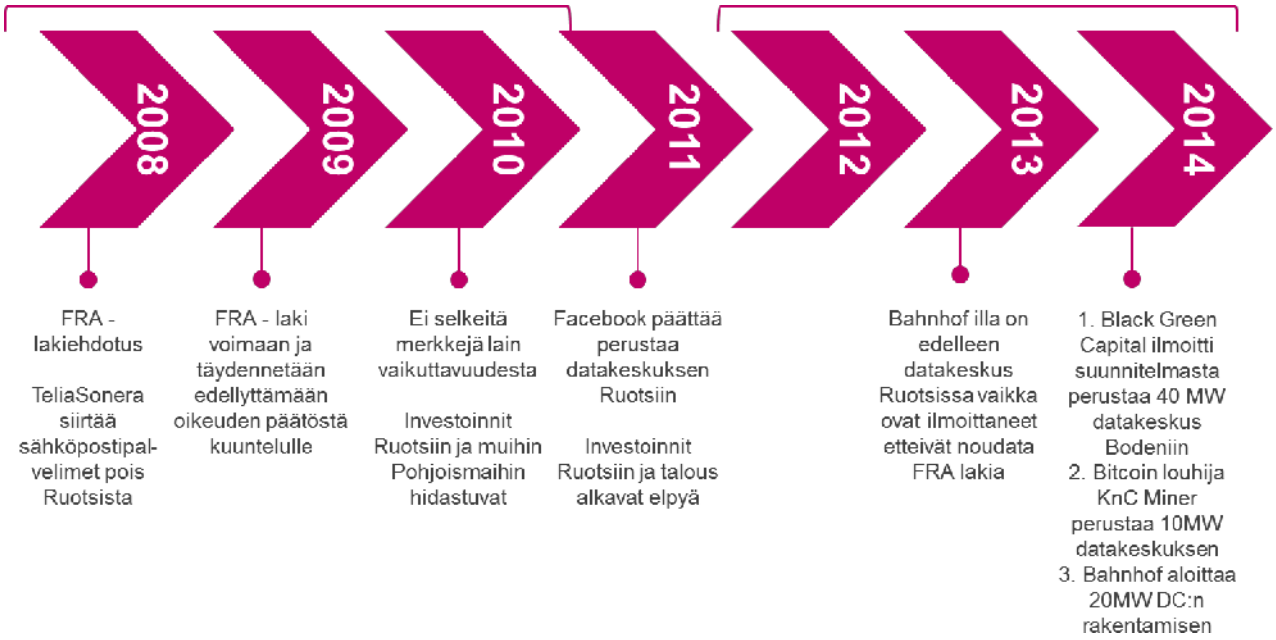
Den starka utvecklingen på ICT-sektorn beskrivs t.ex. av det stora datacenter som Facebook har grundat. Vid den tidpunkt då det ursprungliga investeringsbeslutet fattades 2010 – 2011 var FRA-lagen i kraft. Facebook har kommenterat frågan om FRA-lagen med att alla stater har sina egna metoder för bevakning av datakommunikationen, vilket gör att en klart ordnad sak inte har någon betydelse med tanke på ett investeringsbeslut.

3.5 Konsekvenser för olika företag eller företagsgrupper i Sverige

I och med uppkomsten av FRA-lagen flyttade TeliaSonera sin e-postserver till Finland år 2008, eftersom den finska lagen förutsätter att brevhemligheten bevaras också i e-postkommunikationen. TeliaSonera flyttade samtidigt över också den svenska e-posttrafiken till datacentren i Finland, men efter detta finns inga mera exakta uppgifter att tillgå om tjänstens produktionsplats och var de data finns som ingår i e-posttrafiken.

FRA-lagen orsakade debatt i Sverige också särskilt bland ICT-infrastrukturaktörerna på vilkas affärsverksamhet lagen kunde ha haft direkta resultatverkningar. Lagens verkliga effekter på affärsverksamheten har emellertid varit små eller inte alls realiserats. Efter Snowden-avslöjandena har företagens allmänna medvetenhet om informationsinhämtning ökat.

3.6 FRA tidsperspektivet i Sverige



2008	2009	2010	2011	2013	2014
FRA-lagförslag TeliaSonera flyttar sina e-postservrar från Sverige	FRA-lagen träder I kraft och kompletteras så att det krävs beslut av domstol för avlyssning	Inga klara tecken på att lagen skulle ha haft någon inverkan Investeringarna i Sverige och de övriga nordiska länderna saktar av	Facebook beslutar grunda ett datacenter i Sverige Investeringarna i Sverige och den svenska ekonomin börjar återhämta sig	Banhof har fortfarande ett datacenter I Sverige fastän bolaget har meddelat att det inte följer FRA-lagen	1. Black Green Capital meddelade att bolaget planerar ett 40 MW:s datacenter i Boden 2. Bitcoin miner kNC Miner grundar ett 10MW:s datacenter 3. Banhof inleder byggandet av ett 20MW:s datacenter

Utgående från tidsperspektivet kan man klart konstatera att efter den första förvåningen och den ovetskap som anknöt till det praktiska genomförandet av lagen har lagen inte påverkat t.ex. datacenterinvesteringarna. Också den nyhetsförmedling som anknöt till de nya FoU-investeringarna år 2014 stöder synen att lagen inte har fått investeringarna att minska. Också företagen investerar kraftigt:

2014-06-17 8:00 - CIO Sweden: ”IT-investeringarna växer snabbare än någonsin”

4 Sammandrag

De starka ställningstagandena och åtgärderna från företagens sida i FRA-lagens beredningsfas har huvudsakligen tystnat. Den nuvarande nyhetsförmedlingen sammanhänger mera med medborgarrättigheterna, NSA-avslöjandena samt den politiska diskussionen om saken och om FRA:s allmänna verksamhet.

Som ett enskilt företag motsätter sig Bahnhof fortfarande öppet att lagen verkställs i företagets egen verksamhet, men upplever klart inte att situationen skadar varken företagets egen eller dess kunders affärsverksamhet. Företaget har kraftigt ökat sin verksamhet i Sverige och håller även på att igångsätta ett nytt stort utbyggnadsprojekt i Stockholm ”Project Green”. Målet är att före utgången av år 2016 ha byggt ett nytt 20MW datacenter och en betydande knutpunkt för datakommunikationen i Stockholms centrum och utnyttja energiproduktionens och nedkylningens synergier i samarbete med Fortum. En inrättning av denna storlek innebär en investering av storleksklassen 200 M€, och en sådan görs inte utan bindande kundkontrakt.

I sammandrag kan det konstateras att ett klart samband med FRA-lagens eventuella konsekvenser för IT-sektorns utländska investeringar efter att lagen trätt i kraft eller skillnader jämfört med motsvarande investeringar i Finland inte har kunnat konstateras utgående från utredningen.

Å andra sidan har det också förekommit en sådan syn att en exakt stiftad lag skapar en mera förutsebar omgivning för alla aktörer inom IT-sektorn. Investeringarna ligger på en pålitligare grund när de gemensamma spelreglerna är kända. Stora internationella företag har också blivit mera medvetna än tidigare om cybersäkerhetens område, och det allmännas spelregler för att bevaka området och hantera attacker är välkomna.

5 Länkar

Länkar i Finland

http://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-1.pdf
http://www.itviikko.fi/uutiset/2014/03/10/teknologia-ala-urkintalaki-saattaa-kostautua-kivuliaasti/20143451/7?pos=related

Länkar i Sverige

http://www.thelocal.se/20070530/7452
http://www.aftonbladet.se/nyheter/article11442895.ab

Länkar i Tyskland

http://www.sueddeutsche.de/digital/bundesnachrichtendienst-aufruesten-fuer-den-cyberkampf-1.2211761

Andra länkar

http://www.itworld.com/article/2845603/german-spy-agency-seeks-millions-to-monitor-social-networks-outside-germany.html#tk.rss news

Kontaktuppgifter
Vesa Weissmann
Gearshift Group Ltd.
Mannerheimintie 16, 4th Floor
FI-00100 Helsinki, Finland
Mobile +358 50 500 2120
Email vesa.weissmann@gearshiftgroup.com
Web www.gearshiftgroup.com

Bilaga 2

HÖRANDE AV INTRESSEGRUPPER OCH SAKKUNNIGA I SAMMANDRAG

1 Beslutet om tillsättande av arbetsgruppen på remiss

Som stöd för sitt arbete sände arbetsgruppen tillsättningsbeslutet på remiss till sju instanser

- Finlands näringsliv
- Electronic Frontier Finland (EFFI) ry
- Centralförbundet för datakommunikation och datateknik FiCom ry
- Finnish Communication and Internet Exchange (FiCix) ry
- Försörjningsberedskapscentralen
- FiSC Finnish Information Security Cluster ry och Teknologiindustrier rf (gemensamt remissutlåtande)

FiCom ry sände dessutom en bakgrundspromemoria till arbetsgruppens förfogande (Företagsvärldens syn på det lagstiftningsprojekt som är förknippat med utvecklandet av säkerhetsmyndigheternas förmåga till informationsinhämtning, version 0.3D, 16.1.2014 på finska).

Remissgivarna ombads presentera sina syner särskilt på arbetsgruppens mål och uppdrag samt på det vilka juridiska och samhälleliga synpunkter borde beaktas i arbetsgruppens arbete.

Remissförfarandet tidsbestämdes till begynnelsefasen av arbetet för att den respons man fick skulle kunna beaktas under arbetets gång.

Remissbegäran, remissutlåtandena och andra ställningstaganden samt ett särskilt sammandrag som gjorts över remissutlåtandena och övriga skriftliga påpekanden som lämnats in till arbetsgruppen har satts ut på försvarsministeriets webbplats.

2 Hearingar av näringslivet och organisationerna

Arbetsgruppen ordnade två hearingar, den ena för näringslivet (29.4.2014) och den andra för organisationerna (6.5.2014). Tyngdpunkten vid hearingarna låg på datatrafikspaning. Arbetsgruppen reserverade en möjlighet för de inbjudna att också lämna in skriftliga ståndpunkter.

En skriftlig ståndpunkt lämnades in av

- F-Secure Oyj
- Nokia Oyj och Nokia Solutions and Networks (gemensam ståndpunkt)
- TDC Oy
- Microsoft Oyj
- Centralhandelskammaren
- Internet-käyttäjät ikuisesti - IKI ry

- Finnish Communication and Internet Exchange (FiCix) ry

Inbjudan, deltagarlistor och program för evenemangen samt de skriftliga ställningstaganden som lämnats in till arbetsgruppen har satts ut på försvarsministeriets webbplats.

3 Bakgrundsevenemang för redaktörer

Arbetsgruppen ordnade 12.3.2014 ett evenemang för redaktörer, där bakgrunden till projektet reddes ut. Vid evenemanget presenterades arbetsgruppens uppdrag och målen för arbetet samt andra omständigheter som skulle beaktas i arbetet.

4 De sakkunniga som arbetsgruppen har hört

Under sitt arbete hörde arbetsgruppen 26 sakkunniga, som representerade med tanke på projektet centrala myndigheter och intressegrupper.

lägesbildskoordinator, enhetschef Jarkko Korhonen, statsrådets kansli
statsrådets säkerhetsdirektör Timo Härkönen, statsrådets kansli
dataadministrationsdirektör Ari Uusikartano, utrikesministeriet
specialsakkunnig Kimmo Janhunen, finansministeriet

direktören för EU:s underrättelseanalyscentrum Ilkka Salmi
EU:s militärunderrättelsechef Georgij Alafuzoff

dataombudsman Reijo Aarnio
professorn i juridik Veli-Pekka Viljanen, Åbo universitet

beredskapschef ICT Christian Fjäder, Försörjningsberedskapscentralen
direktör Kirsi Karlamaa, Kommunikationsverket
säkerhetsregleringsgruppens chef Jarkko Saarimäki, Cybersäkerhetscentret
informationssäkerhetsexpert Tomi Hasu, Cybersäkerhetscentret
chefen för Centralkriminalpolisen, polisrådet Robin Lardot
kriminalkommissarie Timo Piiroinen, Centralkriminalpolisen
systemsakkunnig Pasi Paunu, Skyddspolisen

Nordic Policy Counsel David Mothander, Google
förvaltnings- och säkerhetsdirektör Vesa Vuoti, DNA Oyj
Head of Special Network Security Krister Kaipio, TeliaSonera Finland Oyj
säkerhetsdirektör Jaakko Wallenius, Elisa Oyj
Platform Strategy Manager Pasi Mäkinen, Microsoft Oy
Vice President Kaisa Olkkonen, Nokia Government Relations
Head of Security Technologies Gabriel Waller, Nokia Solutions and Networks
forskningsdirektör Mikko Hyppönen, F-Secure Oyj
teknologiedirektör Kimmo Kassin, F-Secure Oyj
smf-direktör Jyrki Hollmén, Finlands näringsliv
Associate Partner Vesa Weissmann, Gearshift Group Oy

5 Sammandrag av intressegruppernas och de sakkunnigas ställningstaganden

5.1 Organiseringen av projektet, dess mål och uppgifter

Vid de hearingar som ordnades, uppmärksammades arbetet som process i den arbetsgrupp som rett ut myndigheternas informationsinhämtning. Framför allt näringslivets representanter betonade att näringslivet måste tas intensivare med i arbetet i de frågor som inte anknyter till myndigheternas behörighetsfördelning eller motsvarande.
En riktad informationsinhämtning i nätet är en känslig sak. Den ska beredas i samarbete också med näringslivet. Oro för att ekonomiska intressen inte är viktiga i arbetet fördes fram. Näringslivet måste kunna lita på myndigheterna liksom också myndigheterna måste kunna lita på näringslivet.

I synnerhet i arbetets begynnelsefas fanns det väldigt knappt med information att tillgå om arbetsgruppens arbete. Det förutsattes att beredningen är öppen, görs på bred bas och är omsorgsfull.

Den tidsfrist på ett halvt år som arbetsgruppen getts ansågs för kort för att genomföra ett samhälleligt betydande projekt med långtgående konsekvenser.

Beslutet om tillsättande av arbetsgruppen väckte debatt liksom också det att beslutet kan tolkas så att arbetsgruppen inte nödvändigtvis har fullmakt att reda ut behoven att inhämta information mera vidsträckt än i fråga om cyberinformationsinhämtning. I målen för arbetsgruppens arbete bör också den privata sektorns uppgift vad gäller upptäckter av cyberhot beaktas.

En granskning av nu gällande lagstiftning ansågs som ett viktigt mål. Enligt en del synpunkter ger lagstiftningen redan nu myndigheterna många olika handlingsmöjligheter. Sådana verksamhets- och övervakningsmekanismer som överlappar eller står i konflikt med varandra bör inte skapas.

En del sakkunniga konstaterade att resultaten av arbetsgruppens arbete inte bör skrivas i form av en regeringsproposition. I den arbetsgruppspromemoria som ska upprättas som grund för det fortsatta arbetet bör den sektorvisa specialregleringen observeras, och vilka verkningar den reglering som gäller informationsinhämtningen har och eventuella begränsningar i tillämpningsområdet sektorvis bör bedömas, till exempel inom sektorerna hälsovårdstjänster och bankverksamhet.

5.2 Internets och kommunikationens karaktär

De sakkunniga betonade Internets och kommunikationens gränsöverskridande karaktär. Flera tjänster som ser inhemska ut produceras i själva verket utomlands. Nationella gränser fungerar inte i Internet, enligt de sakkunniga. Dessutom blir molntjänsterna mera allmänna och det är inte längre så viktigt var informationen finns fysiskt.

På Internet rör sig en ofantlig informationsmängd och den mängden ökar hela tiden. Av denna anledning är det utmanande tekniskt och ekonomiskt att ordna en övervakning som täcker allt. Vid hearingarna funderade man också på att Internet har varit i bruk redan i 20 år, men att de problem som hänger samman med det reds ut först nu.

5.3 Informationssäkerhetens nivå och utvecklandet av den

Vid hearingarna togs det upp att Finlands rykte som ett land med ett bra dataskydd är omstritt. Till exempel företagsvärlden är inte i sin helhet väl skyddad, utan det finns en ofantlig mängd system där man inte har förberett sig på att någon kan attackera dem via nätet. Generellt tänker man att Finland är ett av världens hederligaste länder. Det är klart att förbrytelser har förekommit, men de har inte kommit ut i offentligheten.

En acceptabel cybersäkerhetsverksamhet är enligt intressegrupperna att man i statsförvaltningens organisationer övervakar den information som kommer in till statens egna informationssystem. Detta gäller t.ex. endast enskilda ämbetsverk med klart avgränsade verksamhetsenheter. Av åtgärderna nämndes t.ex. brandväggar, anskaffning av säkra programvaror och intern dataskyddspraxis för organisationens dagliga verksamhet. Allt detta är möjligt redan med stöd av dagens lagstiftning.

Vid hearingarna betonades det också att företagen själva bör sörja för nivån på sitt dataskydd, myndigheternas resurser räcker inte till för detta. Alla måste förbereda sig på cyberhot. De enskilda aktörerna kan kanske bäst upptäcka misstänkt verksamhet i sin nätkommunikation.

Enligt de sakkunnigas åsikt måste staten ha en möjlighet att aktivt försvara sig mot cyberattacker för att kunna skydda försörjningsberedskapen och andra kärnfunktioner. När cyberförsvaret planeras måste man emellertid förstå att cybersäkerhetsverksamhet som starkt betonar ett reaktivt upptäckande av en attack och en aktiv begränsning av attacken är mera riskfyllt med tanke på realiserandet av de grundläggande fri- och rättigheterna än en förebyggande strategi som betonar systemens attacktålighet.

Ett reaktivt upptäckande av attacker och nätunderrättelse förutsätter att kommunikationen följs och profileras i realtid. En proaktiv utökning av systemens attacktålighet igen koncentrerar sig på att förbättra systemen när de utvecklas varvid den ökade informationssäkerheten i systemen samtidigt också ökar deras dataskydd.

Reaktivt upptäckande och aktiva motåtgärder hjälper inte nödvändigtvis i en verklig konfliktsituation, eftersom attackeraren kan utnyttja nolldagssårbarheter, som antingen inte upptäcks eller vilkas verkningar är för snabba för att man skulle hinna reagera på dem ens med automatiskt adapterade metoder. Olika övervaknings- och avvärjningssystem är emellertid affärsverksamhet för de företag som bjuder ut dataskyddsprodukter. Den lobbning som främjar dem är därför hetare än främjandet av en säker utveckling av programvarorna, som inte nödvändigtvis skulle kräva stora investeringar i systemen men desto mera i utbildning och processer.

Proaktivt säkerhetsarbete, t.ex. arbete enligt kraven i den nyaste anvisningen om säkerheten i utvecklandet av VAHTI-tillämpningen (1/2013) skulle effektivera systemens passiva försvarbarhet och minska risken för nolldagsattacker. Om man gav utvecklandet av programvarorna och säkerheten i tillämpningsutvecklingen en strategiskt större roll skulle det sannolikt vara bra för realiserandet både av de grundläggande fri- och rättigheterna och en bättre cybersäkerhetssituation.

Det finns också ett behov att förbättra det informationsutbyte mellan myndigheterna som anknyter till datasäkerhetsintrång. Vidare borde myndigheterna kunna berätta för företag och privatpersoner hurdana attacker som är på gång för att dessa ska kunna skydda sig mot dem. Samtidigt måste man

beroende på hur allvarliga fallen är kunna ålägga offren för attackerna att rapportera om de attacker och tekniker som de blivit föremål för så att andra kan skydda sig mot dem.

I fråga om HAVARO-systemet konstaterades det att det är i funktion och har visat sin användbarhet. Enligt de sakkunniga torde systemet kunna utvecklas så att det bättre lämpar sig för behoven av underrättelseinformation. Ibruktagande av systemet vidsträckt inom den offentliga förvaltningen bör främjas. Med hjälp av HAVARO-systemet eller de monitoreringssystem som kan fås kommersiellt är det möjligt att inrikta underrättelsen så att sådan kommunikation som inte har något underrättelsevärde eller kränker den allmänna rättskänslan inte oskäligt blir föremål för underrättelsen. Inriktningen av underrättelsen gör det också möjligt att utföra en kostnadskontroll mycket exakt och optimalt.

HAVARO-tjänsterna kommer enligt Försörjningsberedskapscentralen att fortgå och förstärkas som en del av Cybersäkerhetscentrets verksamhet. Tjänsterna CERT-FI och HAVARO breddas så att de också täcker statsförvaltningens gemensamma ICT-tjänster.

5.4 Finland som informationens skyddshamn

Vid hearingarna framhävdes det att Finland i den digitala världen kan vara garant för cybersäkerhetens tillförlitlighet. En viktig nationell vision är att skilja sig ur mängden som en framtida knutpunkt för datakommunikationen, ett ”Data-Schweiz” som behandlar internationell datakommunikation mycket konfidentiellt och hos vilken man tryggt kan spara information. I Finland finns mycket teknologi som det är möjligt att utnyttja när denna vision realiseras.

Världens brist på förtroende för de nuvarande aktörerna har öppnat ett tomrum på marknaden, där Finland har obegränsade tillväxtmöjligheter. Möjligheten stöds också av de planerade sjökabelprojekten, vilkas centrala syfte är att göra det möjligt för dataintensiv industri att etablera sig i Finland.

Den utveckling som realiserats ute i världen har skapat en möjlighet för Finland att agera som en rättsstat i cybervärlden. Genom att handla rättvist samt genom att försvara privatpersoners och företags rättigheter och oberoende kan Finland skilja sig ur mängden som ett intelligent digitalt samhälle och som en världsledande koncentration av säker teknologi och företagsamhet.

I arbetsgruppens arbete måste man kunna undvika en sådan situation där Finland marknadsförs som en säker, stabil, förutsebar omgivning, och när etableringsbesluten väl är fattade, tar man i Finland i bruk sådana förfaranden som företagen ville undvika och därför lät bli att etablera sig i konkurrentländerna.

Vid hearingarna funderade man också på om ”Finland som skyddshamn” avser att i Finland är man skyddad mot myndigheterna, som i dagens läge inte har tillräckligt med befogenheter. Också en exakt reglerad nätövervakning kan vara en konkurrensfördel.

5.5 Om konsekvenserna för företagsverksamheten

De sakkunniga betonade att myndigheternas nya befogenheter gällande informationsinhämtningen, om de blir verklighet, i praktiken påverkar olika företag på olika sätt. Företagen bör inte dras över en kam. Verkningar som gäller kostnaderna får i synnerhet teleoperatörerna.
Kostnaderna är avgörande i investeringarna och de påverkar direkt vilket land ett företag väljer för sin etablering. Hela världen är nu för tiden ett marknadsområde. Kostnaderna bör redas ut på förhand så exakt som möjligt och det bör även beslutas vem som svarar för dem.

Det bör observeras att informationsinhämtningen riktar sig mot privat egendom. Företagen måste ge sitt samtycke till verksamheten. Informationsinhämtning är inte teleföretagens näringsverksamhet. Sektorn ska inte behöva bära kostnaderna av detta och inte heller det juridiska eller moraliska ansvaret.

Dataskyddsföretagens löfte till sina kunder lyder ”we will protect you” och detta baserar sig på förtroende för att företagen i fråga strävar efter att garantera att kommunikationen är konfidentiell. Det kan ses att myndigheternas befogenheter att inhämta information kommer att äventyra detta förtroende.

Förutom direkta verkningar måste man också beakta de föreställningar utgående från vilka konsumenterna och företagen väljer sina tjänster. Risken för Finlands rykte måste man vara medveten om. Det får inte uppkomma en uppfattning om att allt övervakas, när man inte föreslår något sådant.
Å andra sidan togs det också upp att förutsebarheten är viktig för investerarna. Finland har varit ett tryggt land och Finland har ett imagevärde som bör skyddas.
Representanterna för de teleföretag som är verksamma i både Finland och Sverige konstaterade för sitt eget företags del att den svenska FRA-lagen inte på något sätt har påverkat verksamheten i praktiken.

5.6 Om myndigheternas behov av befogenheter

Enligt de kommentarer som erhållits bör man utöka den riktade bevakningen av den nätkommunikation som går ut från Finland och anknyter till kriminell verksamhet. Det konstaterades att det enligt den nuvarande lagstiftningen inte är möjligt att gallra ut den kommunikation det är fråga om, utan alla fall behandlas enskilt. Till exempel beteendet hos de skadeprogram och andra tekniker, som nätkriminella och statliga aktörer använder, grundar sig ofta på aktiva datakommunikationsförbindelser över landets gränser. Tekniskt skulle det vara möjligt att upptäcka och rikta i sig på nätkommunikation med anknytning till denna verksamhet utan att innehållet i kommunikationen eller hela den finska interna nätkommunikationen behövde bevakas.

Det ansågs ytterst viktigt att myndighetsverksamheten är genomsynlig och detta hör också till den finska kulturen. Det som myndigheterna gör måste ärligen ges alla för kännedom. Det konstaterades också att de finska myndigheternas verksamhet i utlandet sannolikt inte är problematisk ur programtillhandahållarnas synvinkel.

I Finland finns redan i dagens läge vidsträckta teletvångsmedel och lagstiftning, men de kanske inte utnyttjas i tillräckligt hög grad.

Om det skapas en ny reglering om myndigheternas informationsinhämtning, bör de uppgifter och befogenheter som gäller myndigheternas informationsinhämtning vara specificerade och tillräckligt exakt avgränsade. Informationsinhämtningen bör ha en klar laglig grund.

I lagstiftningen ska det också definieras vilken kommunikation som är skadlig. Över huvud taget bör en eventuell lagstiftning vara exakt. Det ansågs att i detta kunde Finland skilja sig från andra länder. I lagen måste man kunna läsa vad myndigheterna får eller inte får göra, genom detta uppkommer förtroende för myndigheternas verksamhet. Även distributionen av informationen och dessa användningsändamål måste avgränsas tillräckligt.

Också myndigheternas resurser togs upp. Sveriges FRA har en budget på 100 miljoner euro och 300 anställda. Man måste vara säker på projektets effektivitet innan det kan genomföras. Övervakning försiggår trots allt redan nu i många länder, också i de som omger Finland.

Även ett sådant alternativ måste övervägas att myndigheten inte skulle ha till uppgift att vara den egentliga tjänsteproducenten, utan myndighetens uppgift skulle vara att skapa ramarna för samverkan och förmedla information av olika slag mellan parterna.

5.7 Massövervakning

Det finns olika synpunkter på massövervakning. Vid hearingarna togs det upp att som massövervakning också anses att informationsinhämtning görs med exakta sökbegrepp i all datakommunikation. Också om man inte rör i den information som står utanför sökbegreppen, är det fråga om massövervakning eftersom övervakningen inte är riktad. Det anfördes också att efter EU-domstolens data retention -dom är det inte längre möjligt att bedriva massövervakning i ett EU-land. Massövervakning kan inte definieras med myndighetsbeslut. Begreppet ”gallring” förstås som massövervakning. Myndigheten ska övervaka allt det, där informationen inhämtas.

Proportionaliteten ansågs vara en viktig sak. Det måste gå att hitta en balans för hur vittomfattande övervakningen får vara. En bevakning som täcker allt är inte allmänt acceptabel.

Massinsamling av information är, enligt de sakkunniga som hördes, de facto inte till hjälp vid avvärjningen av cyberhot, utan är ett reaktivt sätt där problemet upptäcks först när hotet redan har realiserats och intrång redan har gjorts t.ex. i konsumentens apparat eller myndighetens nät.

5.8 Bakdörrar och nycklar för kryptoforcering

Möjligheten till bakdörrar, dvs. att en myndighet kan ta sig in i en dator, programvara eller motsvarande utan att användaren vet om det, ansågs problematisk och det togs upp att uteslutandet av denna möjlighet ur myndigheternas metodutbud understöds. Likaså ansågs det viktigt att företagen inte åläggs att skapa bakdörrar och till myndigheterna överlåta nycklar med vilka meddelandenas kryptering kan forceras. Båda möjligheterna skulle enligt de sakkunniga betydligt försvåra företagsverksamheten, eftersom konsumenternas förtroende för företagens produkter skulle äventyras.

5.9 Integritetsskyddet, skyddet för förtrolig kommunikation och källskyddet

Integritetsskyddet är en viktig rättighet, när myndigheternas rätt till informationsinhämtning bedöms. Det bör också observeras att människor trots detta överlåter mycket information om sig själva till företag på internet, t.ex. i de sociala medierna.

I fråga om integritetsskyddet konstaterade organisationerna också att integriteten är ett grundläggande värde; staten får inte samla in information, om en människa är oförvitlig och handlar oklanderligt. Information får inte samlas in, också om den varken analyseras eller granskas. Redan genom att informationen samlas in, kränks integriteten.

De sakkunniga tog upp att artikel 7 (Respekt för privat- och familjelivet) och artikel 8 (Skydd av personuppgifter) i Europeiska unionens stadga är av betydelse.
Vid hearingarna konstaterades att kommunikationstjänsternas användares förtroende för att kommunikationen är konfidentiell inte får försvagas utan särskilt vägande motiv. Eventuell nätspaning (torde avse datatrafikspaning) skulle innebära en betydande ändring i det finska rättssystemet och detta kunde smula sönder användarnas förtroende för de kommunikationstjänster och andra tjänster som finska aktörer erbjuder.

Vid hearingarna framfördes ställningstaganden om att det vid informationsinhämtningen inte ska finnas en möjlighet att bryta journalisternas källskydd. I källskyddet betonas förtroende, som inte får äventyras.

Det är svårt att på underrättelse tillämpa grundlagsutskottets etablerade tolkningspraxis gällande skyddet i fråga om hemligheten i ett förtroligt meddelande. Man måste beakta doktrinen om att undantagslagar bör undvikas. Om målet är att skapa ett bestående arrangemang, räcker det inte med ett förfarande med en undantagslag, utan formuleringen i 10 § 3 mom. i grundlagen måste bedömas på nytt. Tolkningsmässigt kan formuleringen inte breddas till underrättelse.

Det måste alltid finnas en godtagbar grund för att begränsa en grundläggande fri- eller rättighet. Till exempel i 10 § 3 mom. i grundlagen förutsätts en konkret brottsmisstanke.
Det ansågs inte fungera att jämställa datatrafikspaning juridiskt med åtgärder som är möjliga för att genomföra dataskydd.

5.10 Konsekvenserna för utrikespolitiken och relationen mellan länder

Vid sakkunnighearingarna kom det fram att förvaringen och hemlighållandet nationellt av känslig information som gäller främmande stater och som erhållits genom underrättelse inbegriper en politisk risk. Internationella händelser under den senaste tiden visar att nationella avgöranden i fråga om nätspaning har omfattande utrikespolitiska konsekvenser.

Eventuella konflikter mellan staterna bör lösas. För att konflikter ska kunna undvikas i lagstiftningen, bör staterna bygga ett ramverk som följer hållbara principer och främjar genomsynlighet för hanteringen av gränsöverskridande informationsbegäranden t.ex. genom att förstärka befintliga överenskommelser om handräckning länderna emellan.

Staterna bör sinsemellan komma överens om de förfaringssätt med vilka de problem som orsakas av eventuella motstridigheter mellan lagstiftningarna i olika länder löses.

5.11 Tillstånd för myndigheternas informationsinhämtning och övervakning av myndigheternas verksamhet

De sakkunniga som arbetsgruppen hörde framhöll att det för verksamheten måste finnas ett mandat i lag och att verkställigheten ska vara beroende av tillstånd.
Informationsinhämtningen bör grunda sig på godtagbara kriterier och hela samhället ska delta i bedömningen av dem (parlamentarism).

De sakkunniga har konstaterat att myndigheternas verksamhet också bör övervakas noga. Ju mera befogenheter, desto effektivare övervakning. Övervakningen måste vara oberoende. Systemet bör vara genomsynligt och kontrollerat samt väcka förtroende. En tillräcklig rådgivningsprocess måste också ordnas.

Eventuella verkställighetsfel ska sanktioneras. Det måste också skapas en skyldighet att ersätta en skada. Eftersom verksamheten bedrivs i hemlighet, ska för parterna skapas en möjlighet att försvara sig, om en person upplever att hen har blivit föremål för osaklig informationsinhämtning. Parterna har inte den information som behövs, utan bevisbördan bör ställas på den myndighet som inhämtat informationen.

Det konstaterades också att om arbetsgruppen beslutar föreslå att rätten att få information breddas, ska arbetsgruppen komplettera de frågor som omfattas av granskningen med utarbetandet av övervakningsmekanismer i fråga om den praxis som hänför sig till informationsinhämtningen. För informationsinhämtningen ska skapas ett effektivt och täckande övervakningssystem, till vilket också hör offentlighetskontroll.

De parter som bistår myndigheterna bör ha rätt att på en allmän nivå offentliggöra uppgifter (t.ex. statistik) om hur de har bistått myndigheterna. Sist nämnda är viktigt i synnerhet med tanke på företagens rättsskydd. Även de finska medborgarna bör få veta hur mycket nätbevakning som görs i vårt land, och hurdana resultat man når med den.

I Finland bör också skapas en handlingsmodell där det alltid kvarstår bevis för myndighetens ageranden vid förebyggandet och utredningen av brott. Med hjälp av bevisen kan det påvisas att inga övertramp har skett eller att man annars har agerat i strid med gemensamma beslut. Genom att handla på detta sätt kan Finland uppnå vidsträckt internationellt förtroende som ett cybersäkert land, i vilket det lönar sig att investera och lagra information tryggt. Det är viktigt att i efterhand kunna bevisa för dem som varit föremål för bevakningen vilken information som har samlats in om dem och vart den har levererats. På detta sätt undviks också långvarigt missbruk och garanteras ett unikt tillfälle till att göra ett riktigt Data-Schweiz av Finland.

Till följd av sakens natur bör de organ som övervakar verksamheten vara självständiga och oberoende. Objekten för övervakningen och mottagarna av begäran om information bör ha möjlighet att besvära sig över besluten.

Myndigheternas och övervakningsorganens centrala beslut bör offentliggöras utan dröjsmål för att medborgarna ska ha möjlighet att övervaka dem.

Det konstaterades att det är viktigt med rapportering om verksamheten. Till exempel Google offentliggör vilka slags informationsbegäranden företaget fått. Det är nödvändigt att företagen får offentliggöra rapporter också i fortsättningen. Också myndigheterna ska rapportera noggrant om sin verksamhet och anföra offentlig statistik. Myndigheterna är skyldiga att offentliggöra den totala mängden informationsbegäranden, detta gör en äkta medborgardebatt möjlig.

5.12 Sammandrag

Allmänt taget ansåg de sakkunniga som arbetsgruppen hörde att det är bra att Finlands nationella cybersäkerhet utvecklas t.ex. genom att den nuvarande regleringen utreds, säkerhetsmyndigheternas behov kartläggs och medborgarnas grundläggande fri- och rättigheter beaktas. I så gott som all er-

hållen respons betonades vikten av en omsorgsfull bedömning av konsekvenserna av utvecklingsförslagen.

I den erhållna responsen uppmärksammades informationssäkerheten och utvecklandet av den i hög grad. Med tanke på förebyggandet av cyberhot är det viktigt såväl för de offentliga som också de privata aktörerna att sörja för datasäkerheten i sina nät bl.a. med tekniska metoder. Informationsutbytet mellan myndigheterna och de centrala aktörerna på verksamhetsområdet bör utvecklas.
Vid hearingarna togs främst ställning till nätövervakningen. Så kallad massövervakning av informationen och installering av bakdörrar i programvarorna motsatte man sig generellt. För att skydda säkerheten ansågs det dock berättigat att vidta motiverade, noga riktade, situationsvisa åtgärder i cyberomgivningen.

Intressegrupperna tog upp att kommunikationstjänsternas användares förtroende för att kommunikationen är konfidentiell inte får försämras utan särskilt vägande motiv. Nätspaning kunde smula sönder användarnas förtroende för de kommunikationstjänster och andra tjänster som finska aktörer bjuder ut. Å andra sidan erkändes det att för att garantera den nationella säkerheten bör myndigheterna ha förutsättningar att bekämpa kriminalitet och hot om terrorism, bara det görs med respekt för individens fri- och rättigheter och kommunikationshemligheten.

I anmärkningarna togs upp aspekter som sammanhänger med de grundläggande fri -och rättigheterna, såsom integritetsskydd och rätt till information, konfidentiell kommunikation, näringsfrihet, egendomsskydd och yttrandefrihet.

Särskilt orolig var man för företagens konkurrenskraft och Finlands rykte som en skyddshamn för information samt för vilka konsekvenser arbetsgruppens förslag kan ha för företagsverksamheten och de investeringar som riktas mot Finland.
Finlands rykte som ett land som respekterar integritetsskyddet är en av den finska IT-industrins konkurrensfördelar som man vill bevara. Finska företags attraktion som investeringsobjekt bör inte skadas.

I de påpekanden som anfördes betonades övervakningen av säkerhetsmyndigheternas verksamhet och en så stor öppenhet som möjligt i den. Ett effektivt och täckande övervakningssystem bör skapas för informationsinhämtningen.

Medborgarna bör få veta hur mycket nätbevakning som utförs och hurdana resultat man når med det. Företagen bör också kunna berätta öppet om de begäranden om information som har riktats till dem.

Representanter för intressegrupperna påtalade att förbättrandet av cybersäkerheten förutsätter samarbete mellan myndigheter och aktörer på den privata sektorn. Allas insats behövs.

TYÖ- JA ELINKEINOMINISTERIÖ
ARBETS- OCH NÄRINGSMINISTERIET
MINISTRY OF EMPLOYMENT AND THE ECONOMY

Bilaga 3

TEM/2491/00.05.01/2013

16 December 2014

Försvarsministeriet

Yttrande på betänkandet från arbetsgruppen för en informationsinhämtningslag

Enligt statsrådets principbeslut av den 24 januari 2013 om en strategi för cybersäkerheten i Finland är ministeriets cybersäkerhetsuppgifter ministeriernas uppgifter som hänför sig till de strategiska uppgifter som har definierats i En säkerhetsstrategi för samhället. Arbets- och näringsministeriet (ANM) svarar som en del av statsrådet bl.a. för verksamhetsmiljön för företagsamheten och innovationsverksamheten i Finland. ANM:s cybersäkerhetsuppgift är bl.a. (3) att stöda näringslivets störnings- och kontinuitetshantering genom ANM:s besluts- och styrarrangemang, att vidta myndighetsåtgärder för att skapa och upprätthålla en investeringspositiv och säker omgivning för företagsverksamheten inklusive utländska servercenter.

Republikens President och statsrådets utrikes- och säkerhetspolitiska ministerutskott diskuterade vid sitt möte den 7 november 2013 bl.a. behoven att utveckla den nationella cybersäkerheten. Som en del av verkställandet av den finska cybersäkerhetsstrategin stakade mötet ut en riktlinje om att arbetet på att utveckla den finska lagstiftningen omedelbart skulle inledas (åtgärd nr 42 i verkställighetsprogrammet och dess förslag till ansvarig part och samarbetsparter). I anknytning till det som sägs ovan tillsatte försvarsministeriet i egenskap av ansvarig part den 13 december 2013 en tjänstemannaarbetsgrupp bestående av samarbetsparter, arbetsgruppen för en informationsinhämtningslag i vars arbete också ANM har deltagit. Arbetsgruppen för en informationsinhämtningslag för i sitt betänkande fram utvecklingsförslag gällande nya behörigheter i fråga om underrättelse, vilka gäller datatrafikspaning och underrättelse i utlandet (personbaserad underrättelseinformation i utlandet och spaning i utländska datasystem).

ANM förstår och godkänner bakgrunden till, målen och uppgifterna för beslutet om tillsättande av en arbetsgrupp för en informationsinhämtningslag liksom också behoven av att övergripande utveckla försvarsmaktens och polisens kapaciteter.

Med tanke på ANM:s ansvarsområde, särskilt de näringspolitiska perspektiven, såsom näringslivets allmänna verksamhetsbetingelser, tryggandet av företagens konkurrenskraft och undvikande av en för stor administrativ börda, de faktorer som påverkar utvecklandet av ett digitalt ekosystem samt främjandet av utländska investeringar är vid sidan av säkerhetspolitiska och medborgarsamhälleliga perspektiv betydelsefulla helheter med tanke på arbetet i arbetsgruppen.

Försvarsministeriet, Finland
Mars 2015

ANM:s utlåtande gäller betänkandets slutsatser och utvecklingsförslag om datatrafikspaning. Till denna del instämmer ANM i kommunikationsministeriets (KM) avvikande åsikt i fråga om punkt 4 i den (Nätövervakning kan ha betydande konsekvenser för företagsverksamheten). I denna punkt konstateras att datatrafikspaning och behörigheten till sådan också kan ha negativa konsekvenser på näringslivets konkurrenskraft och inriktningen av investeringar. Till exempel i statsminister Stubbs regeringsprogram har som mål ställts att Finland ska utvecklas till ett internationellt datakommunikationscenter, varvid det med tanke på uppnåendet av målet är fråga om Finlands förutsättningar att klara sig i konkurrensen om utländska investeringar. Statsministern har också konstaterat att den lagstiftning som gäller cybersäkerheten kommer man att granska i nästa regeringsprogram och under nästa regeringsperiod.

ANM anser följaktligen att till följd av temats stora näringspolitiska och övriga samhälleliga betydelse är det först genom ett mera vidsträckt beredningsarbete med en bredare bas än tjänstemannaarbetsgruppen, i vilket utöver egentliga medlemmar också representanter för näringslivet deltar, möjligt att på ett trovärdigt sätt granska, bedöma och ta ställning till förhållandet mellan fördelarna och nackdelarna med datatrafikpaning samt utgående från detta dra egentliga slutsatser och komma med förslag om hur lagstiftningen ska utvecklas.

I egenskap av ANM:s utnämnda medlem i arbetsgruppen för en informationsinhämtningslag

Kari Mäkinen
personal- och förvaltningsdirektör, beredskapschef

POLIISI
POLIISIHALLITUS

Statement ID-1555035541 114 (125)

16 December 2014 POL-2014-16707

Bilaga 4

Till försvarsministeriet

Polisdirektör Tomi Vuoris yttrande på betänkandet från arbetsgruppen för en informationsinhämtningslag

Försvarsministeriet tillsatte den 13 december 2013 den arbetsgrupp som nu avlåter sitt betänkande. Arbetsgruppen fick till uppgift att utveckla Finlands lagstiftning särskilt i fråga om den lagstiftning som gäller säkerhetsmyndigheternas informationsinhämtning. Som mål ställdes att man i Finland skulle sträva efter att bättre sörja för den nationella säkerheten i synnerhet för att avvärja hot som förekommer i datanäten. I arbetsgruppens sammansättning ingick representanter för centrala myndigheter inom såväl den inre som den yttre säkerheten liksom också representanter för de övriga ministerier till vilka i statsrådets verksamhetsområdesindelning hör ärenden inom området för arbetsgruppens uppdrag.

Säkerhetsutvecklingen under de senaste åren har präglats av att gränsdragningen mellan traditionella militära och civila hot har blivit diffusare. I Finland visar sig detta bl.a. i det att man har tagit i bruk en vidsträckt säkerhetsuppfattning. I synnerhet när det är fråga om hot som riktar sig mot datanäten är det åtminstone i begynnelsefaserna ofta omöjligt att säga vilken arts hot det är frågan om. Det är mycket viktigt att säkerhetsmyndigheterna får en tillräcklig lägesbild också om man rör sig i en gråzon utanför den traditionella hotmodellsuppdelningen.

Syftet var att arbetsgruppens arbete skulle inrikta sig uttryckligen på datanätshot, som också kallas cyberhot. Delvis omlott med arbetsgruppens arbete dryftades Skyddspolisens administrativa ställning och befogenheter i ett projekt som hade tillsatts av minister Päivi Räsänen. Till den del som man i arbetet i den arbetsgrupp det är fråga om här i ett senare skede beslöt fundera också mera omfattande på befogenheter till underrättelse utomlands, som inte hör till datanäten, anser jag att jag har varit bunden vid slutresultatet av inrikesministeriets ovan nämnda projekt i synnerhet av den orsaken att polisens representant i den gruppen var min chef polisöverdirektör Mikko Paatero och även därför att denna sak inte hörde till denna arbetsgrupps ursprungliga uppdrag.

Digitaliseringen genomsyrar samhällets olika funktioner. Samtidigt som tjänsterna flyttar ut i datanäten flyttar tyvärr också hoten dit. Denna utveckling är emellertid oundviklig. I sakkunnighearingarna har det starkt tagits fram å ena sidan behovet att trygga människors, företags och även mera vidsträckt hela samhällets verksamhetsmiljö mot de hot som finns i datanäten, men å andra sidan har det också framhävts att friheten till kommunikation är viktig. Därmed är uppgiftsgivningen ytterst aktuell men samtidigt mycket svår. Slutresultatet bör vara ett system där de grundläggande fri- och rättigheterna beaktas, men med vilket alla skyddas mot såväl interna som externa säkerhetshot.

Arbetsgruppens uppdrag gäller inom inrikesministeriets förvaltningsområde i princip bara polisen, inklusive Skyddspolisen. Justitieministeriet och inrikesministeriet tillsatte den 12 mars 2007 en kommission (förundersöknings- och tvångsmedelskommissionen) som fick till uppgift att bereda en totalrevidering av förundersökningslagen, tvångsmedelslagen och polislagen. Avsikten var att ägna särskild uppmärksamhet åt bl.a. efterspaning i eller via datanät. Egentligt prioritetsområde var polisens och övriga lagövervakningsmyndigheters informationsinhämtning i datanäten däremot inte. Saken diskuterades nog i kommissionen, men först efter att det betänkandet hade avlåtits (Justitieministeriet, Kommittébetänkande 2009:2) den 17 april 2009 har den tekniska och samhälleliga utvecklingen gjort det uppenbart att nu behöver man målmedvetet sätta sig in i också denna sak. Undertecknad var den enda medlemmen i kommissionen av medlemmarna i den arbetsgrupp som nu avlåter sitt betänkande. Den nya förundersökningslagen, tvångsmedelslagen och polislagen trädde i kraft vid ingången av år 2014. Polisens nuvarande – också Skyddspolisens – hemliga informationsinhämtning baserar sig på detta lagpaket.

I fråga om arbetet i den arbetsgrupp som nu avlåter sitt betänkande kan jag konstatera att vid polisen förstår man också mera vidsträckt väl de grunder på vilka man på försvarsministeriets förvaltningsområde har påbörjat arbetet. För förnyandet av Skyddspolisens behov av informationsinhämtning, till de delar som de avviker från den övriga polisens situation, finns det också goda grunder. Även om det finns drag som klart skiljer åt den inre och den yttre säkerheten, är det i sista hand dock fråga om en helhet som kan disponeras utgående från en bred säkerhetsuppfattning. Utgående från det arbete som gjorts i arbetsgruppen verkar det som om lösningsmodellerna för frågan lagstiftningsmässigt kan vara olika för polisen och försvarsmakten. Detta gäller också en del av Skyddspolisens uppgifter. Frågeställningen beror på att det i regel vid datanätshot – även om detta inte riktigt alltid är fallet – är fråga om misstanke om brott. Polisen är den myndighet som har den allmänna behörigheten i brottsbekämpning.

De myndigheter som svarar för säkerheten har ett helt befogat behov att få information från datanäten i anknytning till avvärjningen av hot som hör till deras verksamhetsområde. Med virusbekämpning eller motsvarande i sig fullständigt nödvändiga tekniska metoder kan datanätshoten inte helt avvärjas. I själva verket står de allra allvarligaste hoten kvar när dessa har åtgärdats. I detta hänseende kan Finland inte heller internationellt vara ett undantag. Självklart är att man här rör sig på ett mycket känsligt område, eftersom det i grund och botten är fråga om var gränsen mellan myndigheternas tillgång på information och integritetsskyddet går. Denna sak avgörs på statsförfattningsrättsliga grunder, om man inte vill gå så långt att man börjar ändra grundlagen i denna sak.

I det fortsatta arbetet bör man enligt min åsikt alltså beakta att försvarsförvaltningens och polisförvaltningens behov att få information möjligtvis kan tillfredsställas med olika förfaringssätt. I detta hänseende utgör Skyddspolisen en vattendelare; en del av dess befogenhetsbrister kan fyllas tillsammans med övriga polisens, en del igen bör granskas i ett annat sammanhang. Inom polisens verksamhetsområde kunde man enligt min uppfattning i denna sak i regel framskrida inom ramen för lagförbehållet i 10 § i grundlagen genom att granska saken i normal ordning för straffprocessuell författningsberedning. Det här är just den sak som på sätt och vis inte kom med i förundersöknings- och tvångsmedelskommissionens arbete, men i fråga om vilken utvecklingen under den allra senaste tiden har visat att det vore nödvändigt att reda ut också den. Det ska betonas att i kommissionens arbete eftersträvade man i mycket vid omfattning att också beakta Skyddspolisens behov att inhämta information.

Såsom redan konstaterats bör en del av Skyddspolisens befogenheter granskas separat från den övriga polisens behov. Detta gäller de fall där det är fråga om annat än (i vid bemärkelse) underrättelse som har sin grund i ett brott, såsom att utföra strategiska bedömningar av fenomen och hot. I dessa situationer kan befogenheten inte basera sig på ett brott på det sätt som beskrivits ovan, eftersom man i dem rör sig utanför lagförbehållet. I vilket fall som helst är det helt uppenbart att också den civila underrättelsen – vid sidan om den militära underrättelsen – i Finland bör ha färdigheter för annan informationsinhämtning än sådan som grundar sig på ett brott.

För polisen är det viktigt att brottsbekämpningshelheten inte spjälkas upp och att befogenheterna gäller alla situationer som förekommer inom polisens verksamhetsområde. Medan arbetsgruppens arbete har pågått har det visat sig att det mera i detalj måste redas ut hur tillräckliga polislagens hemliga tvångsmedel är på detta område och vilka nya underrättelsebefogenheter som behövs konkret. Jag vill uppmärksamma att man i samband med beredningen av betänkandet från arbetsgruppen för en informationsinhämtningslag inte har kunnat ge tillräcklig tyngd åt en gestaltning av den helhet som brottsprocessen och brottsbekämpningen bildar. Underrättelse är en metod för inhämtning av information och därmed ur polisens synvinkel en del av brottsbekämpningen som helhet.
Det verkar som om polisens behov – denna gång alltså Skyddspolisen delvis exkluderad – av en effektivare informationsinhämtning i datanäten kunde tillgodoses inom ramen för grundlagen genom att brottsrekvisiten och kriminaliseringen av förberedelsegärningar till dem granskades. Kriminaliseringen av brott som äventyrar samhällets säkerhet kunde kanske breddas i likhet med terroristbrotten. I vissa förberedande brott har planering, rekrytering och motsvarande åtgärder kriminaliserats, medan igen i andra har förutsatts konkreta gärningar, såsom anskaffning av olika varor eller vapen eller motsvarande åtgärder. Det är uppenbart att man på detta sätt inom ramen för lagförbehållet kunde trygga informationstillgången på grundvalen av brott också i de situationer där ett misstänkt brott inte ännu kan härledas till en viss person (okänt hot), men där det finns ett sådant bevis för planering av ett brott i dess begynnelsefas eller för en motsvarande begynnelsegärning att man kan ge tillstånd till informationsinhämtning.

Det är bråttom med att effektivera polisens informationsinhämtning för nätbrottsbekämpning utgående från ett brott. Beredningen av en lagstiftning som möjliggör denna

informationsinhämtning och genom vilken alltså också en del av Skyddspolisens behov av befogenheter skulle tillgodoses, borde kunna inledas utan dröjsmål.

Tomi Vuori
Polisdirektör