**Regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation, 29 § i lagen om behandling av personuppgifter inom Försvarsmakten och 22 § i lagen om behandling av personuppgifter i polisens verksamhet**

## PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att lagen om tjänster inom elektronisk kommunikation, lagen om behandling av personuppgifter inom Försvarsmakten och lagen om behandling av personuppgifter i polisens verksamhet ändras. Det föreslås ändringar som möjliggör ett smidigare informationsutbyte mellan myndigheterna vid sådana kränkningar av informationssäkerheten som är betydande med tanke på samhällets vitala funktioner och vid hot om sådana kränkningar. Enligt förslaget ska den handräckning som Försvarsmakten och polisen lämnar Transport- och kommunikationsverket utvidgas till att gälla betydande kränkningar av och hot mot informationssäkerheten. Därtill föreslås bestämmelser om rätten för en kommunikationsförmedlare att på eget initiativ lämna ut information om meddelanden och förmedlingsuppgifter till Transport- och kommunikationsverket för att kränkningar av informationssäkerheten ska kunna utredas eller förebyggas.

Lagarna avses träda i kraft den 1 februari 2023.

_____

**INNEHÅLL**

## MOTIVERING

# 1 Bakgrund och beredning

## 1.1 Bakgrund

Bakgrunden till regeringens proposition är statsrådets principbeslut om en förbättring av informationssäkerheten och dataskyddet inom kritiska samhällssektorer, som utfärdades den 10 juni 2021. I principbeslutet uppräknas 37 åtgärder som syftar till att förbättra informationssäkerhetens och dataskyddets nivå och identifiera säkerhetshelhetens betydelse för tjänsternas kvalitet och säkerhet i det digitala samhället. Den första åtgärden i principbeslutet är att skapa en gemensam författningsgrund för myndigheternas samarbete i situationer där informationssäkerheten har kränkts, vilket propositionen är en följd av. Avsikten är också att bedöma informationsutbytet mellan myndigheterna samt bestämmelserna om handräckning samt bedöma om nuvarande samarbetsförfaranden som har konstaterats fungera bra bör förstärkas och bedöma samarbetet med den privata sektorn. Denna åtgärd genomför principbeslutets politiska riktlinje att myndigheterna bör samarbeta samt bistås och förstärkas av Cybersäkerhetscentret vid Kommunikationsverket. Genom propositionen genomförs skrivelsen i regeringsprogrammet om en trygg rättsstat och förstärkande av säkerhetsmyndigheternas funktionsförmåga.

Dessutom svarar propositionen på den förändrade säkerhetsomgivningen och på hur den reflekteras i cyberomgivningen. Hoten i cyberomgivningen har blivit mer komplicerade och ökat i synnerhet på grund av digitaliseringen av samhällets olika sektorer. Såsom det konstateras i redogörelsen om förändringarna i den säkerhetspolitiska miljön (SPR 1/2022 rd) intensifieras samarbetet och informationsutbytet mellan civila och militära myndigheter ytterligare för att effektivt förstärka avvärjningen av hoten. Det behövs en rättidig, heltäckande och delad lägesbild för att förutsäga cyberhot och observera cyberavvikelser i ett så tidigt skede som möjligt. De är en förutsättning för att ett angrepp ska kunna stoppas och dess verkningar begränsas.

Propositionen är en del av en större helhet som syftar till att utveckla cybersäkerheten, vars syfte är att avhjälpa sådana direkta brister i lagstiftningen som kan anses nödvändiga för att möjliggöra samarbete mellan myndigheterna för att utreda kränkningar av informationssäkerheten som är betydande med tanke på samhällets verksamhet. Till dataskyddssituationer ansluter sig också mera omfattande frågor som gäller t.ex. myndigheternas uppgiftsfält eller bildandet av omfattande förståelse av en situation. De kräver mera omfattande utredningar och lösningar av dem söks i inrikesministeriets och försvarsministeriets pågående utredningsprojekt om myndigheternas verksamhetsförutsättningar i cybersäkerheten. Uppgifter om projektet finns på statsrådets projektsida under koden PLM003:00/2022.

## 1.2 Beredning

Regeringspropositionen har beretts i en arbetsgrupp, där kommunikationsministeriet, inrikesministeriet. försvarsministeriet, finansministeriet och statens cybersäkerhetsdirektör varit representerade. Uppgifterna om arbetsgruppen finns på statsrådets projektsida under koden LVM71:00/2021. Arbetsgruppen har utfört sitt arbete i form av en regeringsproposition. Arbetsgruppens mandatperiod är 1.2.2022 – 31.3.2023.

Arbetsgruppen har under sitt arbete hört de myndigheter som är centrala med tanke på projektet, såsom Transport- och kommunikationsverket, Cybersäkerhetscentret, polisen, skyddspolisen, Försvarsmakten, Statens center för informations- och kommunikationsteknik Valtori samt de nationella tillsynsmyndigheterna för kritiska sektorer som definieras i EU:s direktiv om åtgärder

för en hög gemensam nivå på säkerhet i nätverks- och in-formationssystem i hela unionen (EU) 2016/1148, nedan NIS-direktivet, dvs. de så kallade NIS-myndigheterna.

Propositionen har bedömts i Rådet för bedömning av lagstiftningen och har genomgått justitieeanslerämbetets förhandsgranskning.

## 2 Nuläge och bedömning av nuläget

### 2.1 De centrala myndigheternas uppgifter vid utredning av kränkningar av informationssäkerheten

Myndighetsansvaret för cybersäkerhet och utredning av kränkningar av informationssäkerheten och hot om sådana har i Finland fördelats mellan olika myndigheter. Varje myndighet har sin egen roll när det gäller störningar i cyberomgivningen och samarbete mellan dessa myndigheter bedrivs kontinuerligt enligt etablerade verksamhetssätt. Med tanke på samarbetet är det viktigt att man kan utbyta information i tillräcklig omfattning för att respektive myndighet ska kunna sköta sin uppgift. Smidigt informationsutbyte är viktigt särskilt i allvarliga fall av dataskyddsintrång där myndigheterna måste agera snabbt för att utreda intrånget och minimera skadorna. Det bedrivs också intensivt samarbete med aktörer inom den privata sektorn, såsom telebolag och dataskyddsexperter, som har en stor betydelse särskilt några det gäller att eliminera skadeverkningarna.

#### 2.1.1 Transport- och kommunikationsverket

I 2 § i lagen om transport- och kommunikationsverket (935/2018) finns bestämmelser om transport- och kommunikationsverkets allmänna uppgifter. Transport- och kommunikationsverket har bland annat till uppgift att främja trafik- och kommunikationssäkerheten samt den tekniska utvecklingen och störningsfriheten inom detta område samt sköta sådana uppgifter inom trafik, transport och elektronisk kommunikation som gäller reglering, tillstånd, godkännanden, register och tillsyn som avser verksamhetsområdet. Dessutom har verket till uppgift att nom den egna verksamheten sörja för beredskapen för störningssituationer under normala förhållanden och för undantagsförhållanden, främja och övervaka funktionssäkerheten i den elektroniska kommunikationen samt inom sitt verksamhetsområde stödja samhällets allmänna beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden.

I 3 § i lagen om transport- och kommunikationsverket finns bestämmelser om transport- och kommunikationsverket Cybersäkerhetscenters uppgifter. Cybersäkerhetscentret har till uppgift att stödja, styra och övervaka informationssäkerheten och tillgodoseendet av integritetsskyddet vid elektronisk kommunikation, upprätthålla en lägesbild över den nationella cybersäkerheten samt främja och säkerställa informationssäkerheten i informationssystem och datakommunikation Cybersäkerhetscentret sörjer för kommunikationsbranschens beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden, främja och övervaka funktionssäkerheten i den elektroniska kommunikationen samt inom sitt verksamhetsområde stödja samhällets allmänna beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden. Cybersäkerhetscentret är nationell NIS-samordningspunkt mellan olika myndigheter.

Det finns bestämmelser om transport- och kommunikationsverkets särskilda uppgifter i 304 § i lagen om tjänster inom elektronisk kommunikation (917/2014, nedan SVPL). Enligt punkterna 1, 7, 9 och 10 i 1 mom. i bestämmelsen har transport- och kommunikationsverket till uppgift att främja den elektroniska kommunikationens funktion, störningsfrihet och trygghet, samt att samla in information om kränkningar och hot om kränkningar av informationssäkerheten för

nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem samt om fel och störningar i kommunikationsnät och kommunikationstjänster. Till de särskilda uppgifterna hör dessutom att utreda orsakerna till störningar av radiokommunikation samt till störningar som en radioutrustning eller teleterminalutrustning orsakar kommunikationsnät, radioutrustningar, teleterminalutrustningar eller elanläggningar. Dessutom har transport- och kommunikationsverket till uppgift att utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem.

### 2.1.2 Polisen

Polisens uppgift är enligt 1 kap. 1 § i polislagen (872/2011) att trygga rätts- och samhällsordningen, skydda den nationella säkerheten, upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning. Desssutom, ska polisen sköta andra uppgifter som uttryckligen föreskrivs i lag samt inom ramen för sina uppgifter ge var och en den hjälp som han eller hon behöver. Polisen utreder brott i datakommunikationsnät och strävar efter att med den information den fått förebygga eventuella kommande brott Polisen upprätthäller den nationella lägesbilden över datakommunikationsbrott.

### 2.1.3 Skyddspolisen

Skyddspolisens uppgift är att på förhand förebygga och bekämpa de allra allvarligaste hoten gentemot den nationella säkerheten, såsom terrorism och främmande staters olagliga underrättelseverksamhet mot Finland. Den har till uppgift att observera, förhindra och avslöja sådana åtgärder, projekt och brott som kan vara ett hot mot stats- och samhällsordningen eller Finlands inre eller yttre säkerhet. Skyddspolisen sköter enligt 1 § i 5 a kap. i polislagen inhämtande av information. dvs. civil underrättelseinhämtning, bland annat för att utreda bakgrunden till och motiven för cyberattacker på nätet för att skydda den nationella säkerheten, stödja den högsta statsledningens beslutsfattande och för att andra myndigheter ska kunna utföra de lagstadgade uppgifter.

### 2.1.4 Försvarsmakten

Försvarsmakten har enligt 2 § i lagen om Försvarsmakten (551/2007) bland annat till uppgift att övervaka landområdena, vattenområdena och luftrummet samt trygga den territoriella integriteten. Försvarsmaktens uppgift är ytterligare att trygga befolkningens livsbetingelser, de grundläggande fri- och rättigheterna och statsledningens handlingsfrihet samt försvaret av den lagliga samhällsordningen, Dessutom är dess uppgift att stödja andra myndigheter, vilket innefattar handräckning för upprätthållande av allmän ordning och säkerhet, för förhindrande och avbrytande av terroristbrott och andra brott som orsakar allvarlig fara för människors liv eller hälsa samt för skyddande av samhället i övrigt. Försvarsmakten ansvarar för Finlands militära cyberförsvar som en del av den nationella cybersäkerheten. Försvarsmakten är skyldig att avvärja datanätsunderrättelse verksamhet som riktar sig mot landets försvar och försvarssystem samt cyberangrepp särskilt då det är fråga om en statlig aktör.

I lagen om militär underrättelseverksamhet (590/2019, nedan militärunderrättelselagen) föreskrivs om Försvarsmaktens underrättelseverksamhet (militärunderrättelse), vars syfte är att till stöd för den högsta statsledningens beslutsfattande inhämta och behandla information om militär verksamhet som riktar sig mot Finland eller som är av betydelse med tanke på Finlands säkerhetsmiljö, inhämta och behandla information till stöd för den högsta statsledningens beslutsfattande om en främmande stats verksamhet eller någon annan sådan verksamhet som allvarligt hotar det finska försvaret eller som äventyrar samhällets vitala funktioner.

Ï lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014) föreskrivs om Försvarsmaktens brottsbekämpning, som omfattar förebyggande och avslöjande av brott samt utredning av sådana brott som omfattas av ett militärdisciplinförfarande. I lagens 9 kap. föreskrivs om uppgifter som gäller förebyggande och avslöjande av brott Till dem hör förebyggande och avslöjande av brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret. Det kan inom landförsvaret vara fråga om exempelvis sådana projekt eller brott som kan hota stats- eller samhällsordningen eller Finlands yttre eller inre säkerhet, såsom landsförräderi. högförräderi, spionage eller olovlig underrättelseverksamhet.

### 2.1.5 Andra centrala myndigheter

Statens center för informations- och kommunikationsteknik Valtori, nedan Valtori) har till uppgift att med stöd av lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013) producera statens gemensamma grundläggande datatekniktjänster samt gemensamma datatekniktjänster som statens verk och inrättningar i princip är skyldiga att använda. Valtoris skyldighet är att se till att verksamheten och produktionen av tjänster fortsätter så störningsfritt som möjligt i störningssituationer i normala förhållanden och i undantagsförhållanden.

I lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015, nedan TUVE-lagen) föreskrivs om säkerhetsnätsverksamheten. Säkerhetsnätet är ett myndighetsnät som ägs och förvaltas av staten. Till det hör ett kommunikationsnät och med det direkt sammanhörande lokaler för anläggningar och anläggningar samt gemensamma informations- och kommunikationstekniska tjänster. Säkerhetsnätet uppfyller kraven på hög beredskap och hög säkerhet i enlighet med vad som särskilt föreskrivs i lag eller bestäms med stöd av lag. Säkerhetsnätet möjliggör daglig verksamhet både för den operativa verksamheten och för de administrativa uppgifterna. Säkerhetsnätets nät- och infrastrukturtjänster produceras av Suomen Turvallisuusverkko Oy (STUVE), som också levererar det i TUVE-lagen avsedda myndighetsradionätet samt myndigheternas tidskritiska mobilkommunikation via bredband. Valtori producerar säkerhetsnätets övriga informations- och kommunikationstekniska tjänster samt integrationstjänster. Den som tillhandahåller nät- och infrastrukturtjänster i säkerhetsnätet ska enligt TUVE-lagen inom sitt uppgiftsområde svara för att de krav på säkerhet, aktionsberedskap, annan beredskap och kontinuitet som gäller säkerhetsnätet uppfylls under normala förhållanden och vid störningar under normala förhållanden samt under undantagsförhållanden. Säkerhetsnätets tjänster är centrala med tanke på förmedlingen av information som utbyts mellan myndigheterna också i störningssituationer vid kränkningar av informationssäkerheten.

Övervakningen av kränkningar av informationssäkerheten enligt NIS-direktivet sköts nationellt av flera olika sektormyndigheter. Tillsynsmyndigheter enligt gällande NIS-direktiv är i fråga om trafik (luftfart, sjöfart, vägtrafik, spårtrafik) och digital infrastruktur samt digitala tjänster Transport- och kommunikationsverket, i fråga om energisektorn Energiverket, i fråga om hälso- och sjukvårdssektorn Valvira, i fråga om finanssektorn Finansinspektionen och vattenförsörjningen NTM-centralen samt jord- och skogsbruks-ministeriet. Varje NIS-myndighet svarar för emottagandet av anmälningar om betydande kränkningar av informationssäkerheten inom sitt verksamhetsområde. Beroende på anmälningssättet går dessa anmälningar inte automatiskt till Cybersäkerhetscentret utan en separat anmälan.

Enligt 12 § 7 punkten i reglementet för statsrådet (262/2003) hör till statsrådets kanslis ansvarsområde statsrådets gemensamma lägesbild, beredskap och säkerhet och den allmänna samordningen av hanteringen av störningssituationer. I lagen föreskrivs om statsrådets lägescentrals uppgifter. Enligt 1 § i lagen om statsrådets lägescentral (300/2017) är lägescentralens uppgift

att för att stödja republikens presidents och statsrådets beslutsfattande och verksamhet samla in och analysera information om säkerhetssituationen och sådana störningar och hot om störningar som äventyrar samhällets vitala funktioner, sköta och koordinera förvaltningsövergripande uppgifter som hänför sig till upprätthållande, sammanställande, samordnande och förmedlande av lägesbilden samt sprida den samordnade informationen till presidenten, statsrådet och andra myndigheter. Dessutom föreskrivs i lagen att ministerierna samt ämbetsverken och inrättningarna inom deras förvaltningsområde ska informera statsrådets lägescentral om olyckor, farosituationer, exceptionella händelser och andra motsvarande störningar till lägescentralen samt om lägescentralens rätt att få information och om överlåtande av sekretessbelagd information.

Statsrådets lägescentral producerar i realtid information om säkerhetsincidenter och en lägesbild som sammanställts av de behöriga myndigheternas information. Lägescentralen kombinerar information från olika myndigheter och öppna källor och rapporterat utgående från dem till statsledningen och olika myndigheter. I detta ingår också sammanställandet av en lägesbild över cybersäkerheten.

### 2.1.6 Utvärdering av myndigheternas uppgifter

På basis av det som beskrivits ovan kan konstateras att det finns flera myndigheter som verkar inom cybersäkerheten och att uppgifterna i någon mån är överlappande. I flera myndigheters verksamhet ingår exempelvis funktioner som gäller utredning av kränkningar av informationssäkerheten, men på grund av uppgifterna skiljer sig målet och syftet med utredningarna från varandra. Transport- och kommunikationsverkets syfte är att utreda kränkningar av informationssäkerheten särskilt från teknisk synpunkt, på så sätt trygga kommunikationens konfidentialitet och också förebygga nya intrång. Polisens intresse av att utreda kränkningar av informationssäkerheten ansluter sig till förebyggande av brott och å andra sidan ställa dem som begått brott inför straffrättsligt ansvar. Skyddspolisens intresse för utredningen gäller i större skala tryggande av den nationella säkerheten och bildandet av en hotbild exempelvis mot statliga aktörer. Försvarsmakten syftar igen genom att utreda brott till att trygga funktioner som hör till landets försvar. Den militära underrättelseverksamhetens mål är att utreda vem som står bakom cyberstörningar särskilt då det är fråga om militär verksamhet samt om vilka intentioner den aktör som står bakom dem har. Metoderna för att utreda cyberstörningar är i stort sett desamma oberoende av myndighet. Den kompetens som behövs för detta finnas således hos flera myndigheter. Endast verksamhetens mål och syfte varierar.

En annan uppgift där myndigheternas uppgifter delvis sammanfaller är upprätthållandet av olika lägesbilder. Till Transport- och kommunikationsverkets uppgifter hör att upprätthålla en nationell lägesbild över cybersäkerheten. Skyddspolisen stöder för sin del denna uppgift genom att producera information för upprätthållandet av lägesbilden. Å andra sidan är Skyddspolisens uppgift också att producera annan information exempelvis som stöd för den högsta statsledningens beslutsfattande. Försvarsmaktens militärunderrättelseverksamhet har motsvarande uppgift när det gäller den militära verksamheten. Polisen upprätthåller en lägesbild över cyberbrottsligheten. De uppgifter som gäller lägesbilden för olika sektorer ansluter sig också till tillsynsmyndigheternas uppgifter inom olika NIS-sektorer. De har till uppgift att allmänt övervaka en viss sektors verksamhet, inklusive de kränkningar av informationssäkerheten som riktar sig mot dem. Valtori svarar för sin del för att den offentliga sektorns system fungerar och följer med deras verksamhet. Den samordnande aktören för de olika lägesbildsinformation är statsrådets lägescentral, vars uppgift är att samla och analysera information om säkerhetsläget och störningar samt hot, som äventyrar samhällets vitala funktioner. Lägescentralen förmedlar informationen vidare för den högst statsledningens beslutsfattande.

I uppgifterna finns enligt det ovan anförda många likheter och i centrum för dessa upp-gifter finns information, som är grund för de åtgärder som myndigheterna vidtar. Myndigheterna har på grund av sina uppgifters karaktär olika metoder för att skaffa information för att sköta sina uppgifter. På grund av syftet med uppgifterna finns det också olika begränsningar och villkor som i vissa situationer skapar utmaningar. I följande avsnitt analyseras närmare den lagstiftning som gäller informationsutbytet mellan myndigheterna och de begränsningar den medför.

## 2.2 Informationsutbyte mellan myndigheterna

Bestämmelser som gäller informationsutbytet mellan myndigheterna finns i lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan offentlighetslagen). Offentlighetslagen tillämpas som en allmän lag, om det inte annanstans i lagstiftningen föreskrivs annorlunda. I 26 § i offentlighetslagen föreskrivs om allmänna grunder för utlämnande av sekretessbelagda uppgifter. Ur en sekretessbelagd myndighetshandling kan en myndighet lämna ut uppgifter om i lag särskilt tagits in uttryckliga bestämmelser om rätten att lämna ut eller att få uppgifter, eller när sekretessplikt har föreskrivits till skydd för någons intressen och denne samtycker till att uppgifter lämnas ut. Enligt 3 mom. i paragrafen får en myndighet lämna ut uppgifter ur en sekretessbelagd handling för handräckning som myndigheten ger samt för något annat uppdrag som myndigheten utfört eller någon uppgift som i övrigt handhas för myndighetens räkning om detta är nödvändigt för att uppdraget eller uppgiften ska kunna skötas. Sekretessbelagda uppgifter kan dock lämnas ut för skötseln av dessa uppdrag eller uppgifter även när det uppenbarligen inte är ändamålsenligt att stryka de sekretessbelagda uppgifterna på grund av deras stora antal eller någon annan jämförbar orsak. Myndigheten ska på förhand försäkra sig om att uppgifterna kommer att hemlighållas och skyddas på behörigt sätt. Myndigheterna får dock enligt 24 § 1 mom. utan någon egentlig bestämmelse utbyta information om sekretessbelagda uppgifter inom ramen för klausulen om skaderekvisit, när informationen inte enligt offentlighetslagen är ovillkorligt sekretessbelagd.

Med stöd av 10 § i förvaltningslagen (434/2003) ska varje myndighet inom ramen för sin behörighet och i den omfattning ärendet kräver på andra myndigheters begäran bistå dessa i skötsel av en förvaltningsuppgift, och även i övrigt sträva efter att främja samarbetet mellan myndigheterna. I förarbetena till förvaltningslagen (RP 72/2002 rd) konstateras att det inte av myndigheternas samarbetsskyldighet kan härledas någon allmän skyldighet att utbyta information utan myndigheterna verkar för att uppfylla uppgifterna inom sitt eget förvaltningsområde, med sina egna befogenheter och inom ramen för sin egen sekretessplikt.

### 2.2.1 Transport- och kommunikationsverket

I 315 § i lagen om tjänster inom elektronisk kommunikation bestäms om myndigheternas allmänna rätt att få information att de myndigheter som övervakar bestämmelserna i lagen när de utför uppgifter enligt lagen har rätt att få den information de behöver för skötseln av uppgifterna av dem vilkas rättigheter och skyldigheter lagen gälle. Dessutom kan de som lagen gäller åläggas att samla in information. Uppgifter om meddelanden, förmedlingsuppgifter och lokaliseringsuppgifter ingår inte i den allmänna rätten att få information. I lagen definieras inte närmare vilka de aktörer är från vilka myndigheterna kan få information, men lagens skyldigheter eller rättigheter har ofta riktats till någon viss aktör. Enligt lagens förarbeten kan rätten att få information i princip gälla vem som helst som lagen gäller.

I 316 § i lagen föreskrivs om behandling och utplåning av uppgifter om kommunikation och lokalisering. Transport- och kommunikationsverket har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att få de förmedlingsuppgifter och

lokaliseringsuppgifter som behövs för utredning av fel och störningar samt oklarheter i faktureringen. Dessutom har verket rätt att få förmedlingsuppgifter, lokaliseringsuppgifter och meddelanden, om de behövs för utredning av betydande kränkningar av eller hot mot informationssäkerheten. Dessutom krävs det för rätten att få information att det enligt verkets bedömning finns skäl att misstänka att något av de brottsrekvisit som nämns i paragrafen uppfylls. Bestämmelsen har i praktiken tolkats så att rätten att få förmedlingsuppgifter och lokaliseringsuppgifter gäller samma aktörer verket har rätt att få information från med stöd av lagens 315 §.

I 318 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om utlämnande av information från myndigheter trots sekretessbestämmelserna. Transport- och kommunikationsverket får lämna ut uppgifter till Energimyndigheten, Finansinspektionen, Val-vira samt NTM-centralen, dvs. till NIS-myndigheterna om det är nödvändigt för skötseln av deras lagstadgade uppgifter i anslutning till informationssäkerhet. Transport- och kommunikationsverket har dessutom rätt att utlämna sekretessbelagda dokument eller uppgifter till finansministeriet om det är nödvändigt för skötseln av uppgifter som gäller erbjudande av nät- och kommunikationstjänster i anslutning till myndighetsnätverket och myndigheternas kommunikation. Rätten att utlämna information gäller enligt 318 § 5 mom. inte information om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter eller om innehållet i och existensen av konfidentiella radiosändningar.

Enligt lagens 319 § 1 mom. är sådana uppgifter som Transport- och kommunikations-verket n med stöd av 316 och 317 § har fått och skaffat om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter samt om innehållet i och existensen av konfidentiella radiosändningar sekretessbelagda. Transport- och kommunikationsverket har enligt 319 § 2 mom. punkt 1 trots sekretessen enligt 1 mom. och andra begränsningar som gäller utlämnande av uppgifter rätt att lämna ut förmedlingsuppgifter och andra uppgifter som verket fått i samband med insamling av information om och utredning av kränkningar av informationssäkerheten till en kommunikationsförmedlare, en leverantör av mervärdestjänster, ett företag, en organisation, en abonnent och en användare, om denna har blivit utnyttjad i samband med kränkningen av informationssäkerheten eller har blivit eller sannolikt kan bli utsatt för en sådan kränkning, och om det enligt Transport- och kommunikationsverkets bedömning finns skäl att misstänka att det har begåtts ett sådant brott som nämns i 316 § 2 mom. 1–12 punkten. Dessutom får information lämnas ut till en sådan i en annan stat verksam myndighet eller annan motsvarande aktör som har till uppgift att förebygga eller utreda sådana kränkningar av informationssäkerheten som är riktade mot kommunikationsnät och kommunikationstjänster. När verket bestämmer vilka myndigheter och andra aktörer som avses ska det samarbeta med kommunikationsministeriet. Verket får lämna ut information endast i endast i nödvändig utsträckning. Det är beaktansvärt att det enligt den nuvarande formuleringen av lagen inte är möjligt att lämna ut information exempelvis till EU eller Nato.

Enligt lagens 322 § föreskrivs det i polislagen och tvångsmedelslagen (806/2011) om polisens rätt att få förmedlingsuppgifter för att förebygga, avslöja och utreda brott. När det gäller Gränsbevakningsväsendets och Tullens brottsbekämpningsverkesamhet finns bestämmelserna i egna lagar.

För närvarande föreskrivs i lagens 275 § om teleföretags skyldighet att göra en anmälan om dess tjänster utsätts för eller hotas av betydande kränkningar av informationssäkerheten eller av någonting annat som gör att en kommunikationstjänst inte fungerar eller väsentligen stör den. På motsvarande sätt har Transport- och kommunikationsverket med stöd av lagens 316 § 2 mom. rätt att begära information om en kränkning av informationssäkerheten som det fått kännedom om. Bestämmelserna är dock oklara när det gäller huruvida teleföretag och andra kom-

munikationsförmedlare vid en kränkning av informationssäkerheten frivilligt och på eget initiativ får lämna ut förmedlingsuppgifter och information om meddelanden till verket, ifall kränkningen inte annars skulle komma till verkets kännedom. Transport- och kommunikationsverket har till uppgift att utreda kränkningar av informationssäkerheten. men enligt lagens 137 § 2 mom. får elektroniska meddelanden och förmedlingsuppgifter lämnas ut endast till aktörer som har rätt att behandla uppgifterna i det aktuella fallet. Den uppgift som föreskrivs i lagens 304 § tolkas dock inte som sådan utgöra någon grund för behandling av förmedlingsuppgifter och innehåll i kommunikation. Det är därför oklart vilken grunden för utlämnande av information till Transport- och kommunikationsverket kunde vara vid utredning av kränkning av kränkning av kommunikationsförmedling i en situation då utlämningen av information görs på eget initiativ och då 275 § inte kan tillämpas eller inte skulle förutsätta att information om kommunikationen ges.

Transport- och kommunikationsverket har på basis av det som beskrivits ovan omfattande rättigheter att få information på tillsynsrättsliga grunder. Rätten att få information om meddelanden, förmedlingsuppgifter och lokaliseringsuppgifter är dock mera begränsad. Verket har dock laglig rätt att får information också om dessa uppgifter i situationer då informationssäkerheten kränkts. Utöver ovannämnda görs också av privata aktörer frivilligt en betydande mängd anmälningar om kränkning av informationssäkerheten, vilka kan innehålla olika uppgifter i anslutning till kränkningar av informationssäkerheten, såsom förmedlingsuppgifter och uppgifter om meddelandens innehåll. Om vidarebefordran av den information som lämnats ut föreskrivs separat och till den ansluter sig vissa begränsningar, särskilt när det gäller meddelandens innehåll, förmedlingsuppgifter och lokaliseringsuppgifter. Begränsningarna gällande dessa uppgifter bygger på skyddet av konfidentiell information enligt grundlagen.

### 2.2.2 Polisen

Den lagstiftning som gäller polisens verksamhet är mångfasetterad, beroende på polisens olika uppgifter. I polislagen finns allmänna bestämmelser om polisens verksamhet, befogenheter och dessutom om hemliga sätt att skaffa information, som polisen kan an-vända för att förebygga och avslöja brott. I polislagen föreskrivs också om civil underrättelseinhämtning som hör till skyddspolisens uppgifter och som kompletteras av lagen om civil underrättelseinhämtning avseende datatrafik (582/2019). Förundersökningslagen (805/2011) tillämpas på förundersökning av brott och på tvångsmedel och informationshämning som används vid förundersökning tilllämpas tvångsmedelslagen. I lagen om behandling av personuppgifter i polisens verksamhet (616/2019, nedan polisens personuppgiftslag) föreskrivs såsom framgår av namnet om polisens behandling av personuppgifter.

I polislagens 4 kap. föreskrivs om polisens rätt att inhämta information. Enligt 2 § i la-gens 4 kap. har polisen oberoende av tystnadsplikten på begäran av en polisman som hör till befälet rätt att för tjänsteuppdrag avgiftsfritt få behövlig information och handlingar av myndigheter och sammanslutningar som tillsatts för att sköta offentliga uppgifter, om inte överlämnande av informationen eller handlingarna till polisen eller användning av informationen som bevis uttryckligen har förbjudits eller begränsats i lag. Enligt tolkningen är 318 § 1–4 mom. i lagen om tjänster inom elektronisk kommunikation ett sådant uttryckligt förbud, eftersom där föreskrivs om de myndigheter till vilka information får utlämnas och polisen inte nämns i detta sammanhang. I förarbetena till polislagen (RP 57/1994 rd, s. 67) konstateras att den rätt att få information som definieras i paragrafen exkluderar sekretessplikt om vilken bestäms annanstans i lag, om inte det i bestämmelsen om sekretessplikt förbjuds att uppgifterna utlämnas till polisen. Förbudet kan uttryckas också genom att räkna upp de myndigheter som har rätt att få information och nämna polisen bland dem. När det gäller information om kommunikation är situationen den här, med undantag för en situation som avses i 319 § 4 mom., som gäller utlämnande av

förmedlingsuppgifter till en annan myndighet om det är nödvändigt för utredning av eller väckande av åtal för ett brott som förorsakats av radiostörningar eller för att eliminera eller begränsa störning av radiokommunikation. Med stöd av 319 § 2 mom. i lagen kan annars till polisen utlämnas information om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter eller om innehållet i och existensen av radiosändningar endast i de fall då polisen själv är föremål för en kränkning av eller ett hot om kränkning av informationssäkerheten.

I polislagens 4 kap. 3 § föreskrivs om polisens rätt att få information av privata sammanslutningar och personer för att förhindra eller utreda ett brott. Polisen har rätt att få information oberoende av att en sammanslutnings medlemmar, revisorer, verkställande direktör, styrelsemedlemmar eller arbetstagare är bundna av sekretessplikt. Bestämmelsen ger inte polisen rätt att få förmedlingsuppgifter eller information om innehållet i ett meddelande eftersom det finns särskilda förutsättningar för att få denna information enligt polis- och tvångsmedelslagen.

Enligt polislagens 4 kap. 3 § 2 mom. har polisen 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. Överensstämmande bestämmelser om teleföretags skyldighet att bistå polisen och om åtkomst till vissa uppgifter finns i bestämmelserna om polisens hemliga metoder för inhämtande av information (Polislagen 5 kap. 61 §), Skyddspolisens civila underrättelseinhämtning (polislagen 5a kap. 51 §) och hemliga tvångsmedel (Tvångsmedelslagen 10 kap. 63 §).

När det gäller myndigheteras utlämnande av sekretessbelagd information är den grundläggande principen bestämmelserna i offentlighetslagen. I praktiken förutsätter detta således att det i lagen finns en särskilt föreskriven grund för utlämnande av information, vilket i praktiken medför utmaningar eftersom det är svårt att på förhand bedöma alla situationer där information utlämnas. Information får dock med stöd av 17 § 3 mom. och 26 § i offentlighetslagen lämnas ut till en begränsad krets, såsom till en annan myndighet inom de gränser som en klausul om skaderekvisit anger enligt 24 § 1 mom. i offentlig-hetslagen.

Om utlämnande av information i enskilda fall föreskrivs i polislagens 7 kap. 2 §. Enligt denna paragraf hindrar inte polisens tystnadsplikt utlämnande av information till en myndighet som på grund av sina lagstadgade uppgifter behöver information om omständigheter som annars är sekretessbelagda. Detta kan betyda exempelvis förmedlingsuppgifter eller information om ett meddelande. I förarbetena till polislagen (RP 224/2010 rd s. 147) konstateras att även om utlämnande av uppgifter i enlighet med 7 kap. 2 § 1 mom. i allmänhet sker på begäran av en annan myndighet är det ändå inte en förutsättning för att bestämmelsen ska kunna tillämpas. Enligt förarbetena kan det för polisen uppkomma situationer där det också är nödvändigt och motiverat att utlämna information till en annan myndighet på eget initiativ. Också i rättslitteraturen har det med hänvisning till förarbetena till polislagen ansetts att begäran från en annan myndighet för utlämnande av de uppgifter som avses i 7 kap. 2 § 1 mom. i polislagen inte är en nödvändig förutsättning utan att utlämnandet av uppgifter kan ske också på eget initiativ. Också biträdande justitieombudsmannen har ansett (EOAK/3813/2017) att det uppenbart är etablerad praxis att polisen på eget initiativ lämnar ut uppgifter, för vilken kan anses finnas grunder i bestämmelsen i 7 kap. 2 § och i förarbetena till denna bestämmelse. Det är dock beaktansvärt att hovrätten i sitt avgörande HO 4.3.2021 nr 263, konstaterar att bestämmelsen i polislagens 7 kap. 2 § inte är en behörighetsbestämmelse med stöd av vilken polisen till utsökningsmyndigheterna på eget initiativ kan lämna ut uppgifter. Ärendet behandlas som bäst av Högsta domstolen. Polislagens bestämmelse om utlämnande av information är primär i förhållande till 22 § i lagen om behandling av personuppgifter i polisens verksamhet.

I 24 § 1 mom. 3 punkten i offentlighetslagen föreskrivs att anmälan om brott till polisen eller någon annan förundersökningsmyndighet, en åklagare eller en kontroll- och tillsynsmyndighet, handlingar som har mottagits eller uppgjorts för förundersökning och åtalsprövning är sekretessbelagda. De uppgifter om vilka föreskrivs i denna punkt är sekretessbelagda om det inte är uppenbart att utlämnandet av uppgifter ur en sådan handling inte äventyrar brottsutredningen eller undersökningens syfte eller utan vägande skäl vållar den som har del i saken skada eller lidande eller hindrar domstolen från att utöva sin rätt att sekretessbelägga handlingar enligt lagen om offentlighet vid rättegång i allmänna domstolar. Enligt 2 kap. 2 § i förundersökningslagen leds förundersökningen av en undersökningsledare och denne beslutar således bland annat under förundersökningens gång om uppgifter ska lämnas ut. I 11 kap. 7 § i förundersökningslagen föreskrivs om information om förundersökning.

Polisen får information för att förhindra och avslöja brott också genom hemliga metoder för inhämtande av information enligt 5 kap. i polislagen och för förundersökning genom hemliga tvångsmedel som avses i 10 kap. i tvångsmedelslagen. Till dessa metoder hör exempelvis teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter samt inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning. Förutsättningen för användning av hemliga metoder för inhämtande av information är att man med den metoden kan antas få information som behövs för förhindrande, avslöjande eller avvärjande av risk för brott. Förutsättningen för användning av hemliga tvångsmedel är att det kan antas att man på det sättet får information som behövs för att utreda ett brott. Hemligt inhämtande av information eller hemliga tvångsmedel ska antas vara av synnerlig vikt för utredning, förhindrande eller avslöjande av ett brott. I polislagens 5 kap. 3 § uppräknas de brott för vilkas utredning hemligt inhämtande av information får användas. Tillstånd för användning av hemligt inhämtande av information och hemliga tvångsmedel ska i princip ansökas hos domstol. I vissa brådskande fall kan beslut temporärt fattas också av en anhållningsberättigad tjänsteman innan man hinner få domstolens beslut i ärendet.

När det gäller hemliga metoder för inhämtande av information föreskrivs i 5 kap. 52 § i polislagen att upptagningar som uppkommit vid hemligt inhämtande av information enligt ett särskilt beslut får undersökas av en annan person som anlitas för inhämtande av information än av polisen. I fråga om civil underrättelseverksamhet finns bestämmelsen i 5 a kap. 43 § i polislagen och i fråga om hemliga tvångsmedel i 10 kap, 54 § i tvångsmedelslagen.

Skyddspolisen får information genom underrättelseinhämtning enligt 5 a kap. i polislagen, vilka är motsvarande som vad som föreskrivits om polisens hemliga metoder för inhämtande av information och om hemliga tvångsmedel. Förutsättningen för användningen av dessa metoder är att användningen av den är nödvändig för att få viktig information om sådan verksamhet som är föremål för civil underrättelseinhämtning och som allvarligt hotar den nationella säkerheten. Om användning av underrättelsemetoder beslutar i cybermiljö i huvudsak en domstol. I vissa brådskande fall kan beslut temporärt fattas också av chefen för skyddspolisen eller en för uppdraget förordnad polisman som hör till befälet vid skyddspolisen och som är förtrogen med användningen av metoder för underrättelseinhämtning innan man hinner få domstolens beslut i ärendet.

I 5 a kap. 44 § i polislagen föreskrivs om i vilka situationer skyddspolisen inte får anmäla samt i vilka situationer skyddspolisen ska anmäla och i vilka situationer den enligt övervägande får anmäla uppgifter som fåtts genom civil underrättelseinhämtning till centralkriminalpolisen. Dessutom föreskrivs i paragrafen om skyldigheterna att anmäla ett brott som ännu kan förhindras. Anmälningsskyldigheten eller – rätten beror på straffbarheten för dem gärning som uppdagats. En sådan anmälan kan göras endast för de allvarligaste brotten. I princip har underrättelseverksamhet skilts åt från uppgifter inom förundersökning och de uppgifter som fås genom

dessa hålls åtskilda eftersom tröskeln för användning av underrättelsemetoder är lägre än för motsvarande metoder inom förundersökning. Det är fråga om så kallad brandmurslagstiftning.

I 5 a kap. 55 § i polislagen föreskrivs om skyddspolisens samarbete med andra myndig-heter och med företag och sammanslutningar. Skyddspolisen ska enligt behov agera i samarbete med andra myndigheter för att den civila underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt. Skyddspolisen får för att genomföra sitt uppdrag avseende civil underrättelseinhämtning trots sekretessbestämmelserna lämna ut andra uppgifter än personuppgifter till andra myndigheter, men också till företag samt andra sammanslutningar, om utlämnandet av uppgifterna behövs för att skydda den nationella säkerheten.

I 14 § i lagen om civil underrättelseinhämtning avseende datatrafik föreskrivs om undersökning av upptagningar som uppkommit vid användningen av underrättelseinhämtning. På motsvarande sätt som i annan underrättelseverksamhet får upptagningarna undersökas endast av domstol eller en polisman som hör till befälet vid skyddspolisen eller av underrättelsetillsynsombudsmannen eller en av denne förordnad tjänsteman. Enligt förordnande av en polisman som hör till befälet vid skyddspolisen eller enligt anvisning av domstolen får upptagningarna undersökas även av en annan polisman, av en sakkunnig eller av någon annan som anlitas för inhämtande av information.

Om utlämnande av information om skadliga datorprogram eller skadliga datakommandon till myndigheter, företag eller sammanslutningar föreskrivs i 16 § i lagen om civil underrättelseinhämtning avseende datatrafik. Skyddspolisen får trots sekretessbestämmelserna lämna ut sådan information som inhämtats med hjälp av underrättelseinhämtning som avser datatrafik och som gäller skadliga datorprogram eller skadliga datakommandon till myndigheter, företag eller sammanslutningar, om utlämnandet av informationen behövs för att skydda den nationella säkerheten eller informationsmottagarens intressen. På utlämnande av information till brottsbekämpning tillämpas vad som i polislagen bestäms om saken.

I 22 § i lagen om behandling av personuppgifter i polisens verksamhet föreskrivs om övrigt utlämnande av personuppgifter till myndigheter. Uppgifter som avses i lagens 5–8, 11 och 12 §, såsom uppgifter som gäller specificering, beskrivningar och klassificeringar i anslutning till polisens uppdrag, åtgärder och händelser får utlämnas till de myndigheter som anges i underpunkterna i 22 § 1 mom. Denna lista är dock inte betydelsefull med tanke på utredning av cyberstörningssituationer, utan i fråga om dem tillämpas 22 § 3 mom. enligt vilket polisen av grundad anledning trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd till en myndighet får lämna ut personuppgifter som är nödvändiga för att utföra en uppgift som i lag föreskrivits för myndigheten. En förutsättning för att uppgifter får lämnas ut är således en nödvändig orsak och en i lag föreskriven uppgift.

Enligt 21 § i lagen om behandling av personuppgifter i polisens verksamhet får polisen trots sekretessbestämmelserna lämna ut sådana personuppgifter som avses i lagen bland annat till skyddspolisen och Försvarsmakten för de uppgifter som myndigheten har enligt 1 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018), nedan dataskyddslagen i brottkålsärenden. Dessa uppgifter kan vara exempelvis förebyggande, avslöjande, utredning eller åtalsprövning av brott,

På grund av polisens omfattande uppgiftsfält är också lagstiftningen om polisens rätt att få information och om utlämnande av information ganska komplicerad. Polisen har allmänt taget för skötseln av sitt uppdrag omfattande allmänna rättigheter att få information, som då situationen så kräver kompletteras av bestämmelserna om hemliga metoder för inhämtande av information och hemliga tvångsmedel. Särskilda begränsningar av polisens rätt att få information ansluter

sig till Transport- och kommunikationsverkets uppgifter om kommunikation. För att få motsvarande uppgifter borde polisen i normala förhållanden använda sina egna metoder för inhämtande av information, vilka förutsätter kontroll av domstol.

Polisens utlämnande av information grundar sig allmänt på offentlighetslagen, men också på bestämmelsen om utlämnande av information i 2 § i 7 kap. i polislagen och å andra sidan på bestämmelserna om utlämnande av personuppgifter i lagen om behandling av personuppgifter i polisens verksamhet. Under en förundersökning överväger undersökningsledaren från fall till fall vilka uppgifter som kan lämnas ut med städ av förutsättningarna i 24 § 3 punkten i offentlighetslagen. I lagstiftningen har också angetts vissa begränsningar för informationsutbytet mellan olika polisenheter, vilket beror på skyddspolisens avvikande roll i den övriga polisorganisationen. Det är närmast fråga om ovan beskrivna så kallade brandmurslagstiftning.

### 2.2.3 Försvarsmakten

Försvarsmakten har med stöd av 17 § i lagen om försvarsmakten rätt att trots sekretessplikten av myndigheter och av sammanslutningar som tillsatts för att sköta ett offentligt uppdrag få de uppgifter och handlingar som är nödvändiga för skötseln av lagstadgade uppdrag, om inte lämnandet av uppgiften eller handlingen till Försvarsmakten eller användningen av uppgifterna som bevis har förbjudits eller begränsats i lag. På utlämnandet av information tillämpas offentlighetslagen.

Enligt 17 § i lagen om militär underrättelseverksamhet ska militärunderrättelsemyndigheterna agera i samarbete med skyddspolisen för att underrättelsemyndigheternas uppgifter ska kunna skötas på ett ändamålsenligt sätt och i detta syfte, trots vad som föreskrivs om sekretess, ge skyddspolisen behövliga uppgifter. Enligt lagens 18 § ska militärunderrättelsemyndigheterna enligt behov agera i samarbete med andra myndigheter för att den militära underrättelseinhämtningen ska kunna skötas på ett ändamålsenligt sätt. Militärunderrättelsemyndigheterna kan för att genomföra sitt uppdrag, trots sekretessbestämmelserna lämna ut andra uppgifter än personuppgifter, om utlämnandet av uppgifterna är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten.

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

Enligt 74 § i militäruuderrättelselagen får militärunderrättelsemyndigheterna trots sekretessbestämmelserna till ett företag, en sammanslutning eller myndighet lämna ut uppgifter som inhämtats med hjälp av underrättelseinhämtning som avser datatrafik och som gäller ett skadligt datorprogram och dess verkningar, om utlämnandet av uppgifterna behövs med avseende på det militära försvaret, för att skydda den nationella säkerheten eller trygga företagets eller sammanslutningens intressen.

I 79 § i militärunderrättelselagen föreskrivs om anmälan om brottsmisstanke till centralkriminalpolisen om det medan en metod för underrättelseinhämtning används framkommer att ett sådant brott kan antas ha begåtts för vilket det föreskrivna strängaste straffet är fängelse i minst sex år. Dessutom får anmälan göras om anmälan kan antas vara av synnerlig vikt för utredningen av ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst tre år Dessutom ska

militärunderrättelsemyndigheterna enligt lagens 80 § utan dröjsmål anmäla till en behörig myndighet, om det medan en metod för underrättelseinhämtning används framkommer att ett sådant brott är på färde för vilket det föreskrivna strängaste straffet är fängelse i minst sex år, och brottet ännu kan förhindras och anmälan får göras det föreskrivna strängaste straffet är fängelse i minst två år. Det är fråga om motsvarande brandmurslagstiftning som tidigare beskrivits i fråga om förhållandet mellan skyddspolisen och centralkriminalpolisen.

I 111 § i militärunderrättelselagen föreskrivs om undersökning av upptagningar som uppkommit vid användningen av metoder för underrättelseinhämtning. Uppgifterna får undersökas endast av domstol, huvudstabens underrättelsechef, en till uppdraget av militärunderrättelsemyndigheterna förordnad militärjurist eller annan tjänsteman eller av underrättelsetillsynsombudsmannen eller en av denne förordnad tjänsteman. På förordnande av huvudstabens underrättelsechef eller enligt anvisning av domstolen får upptagningar också undersökas av en annan än en ovan avsedd tjänsteman vid en militärunderrättelsemyndighet, en sakkunnig eller en annan person som bistår vid inhämtande av information.

Enligt 29 § i lagen om behandling av personuppgifter inom Försvarsmakten (332/2019, nedan Försvarsmaktens personuppgiftslag) får Försvarsmakten trots sekretessbestämmelserna till en annan myndighet och till en sammanslutning som tillsatts för att sköta ett offentligt uppdrag lämna ut personuppgifter som behövs för fullgörande av dess lagstadgade uppgifter. I paragrafen uppräknas myndigheter och uppgifter för skötseln av vilka uppgifter får lämnas u. Uppgifter får för det första lämnas ut till polisen för de uppgifter enligt 1 kap. 1 § 1 mom. i polislagen vilka sammanhänger med att trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning, Dessutom får uppgifter lämnas ut till Cybersäkerhetscentret vid Transport- och kommunikationsverket för skötseln av uppgifter enligt 3 § i lagen om Transport- och kommunikationsverket. Detta omfattar exempelvis upprätthållandet av den nationella lägesbilden samt främjande av informationssäkerheten för informationssystem och elektronisk kommunikation. I paragrafen hänvisas dock inte exakt till alla de särskilda som Cybersäkerhetscentret i praktiken ansvarar för enligt 304 § i lagen om elektronisk kommunikation och till vilka hör bland annat att utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem.

Försvarsmakten får med stöd av 30 § i Försvarsmaktens personuppgiftslag utöver vad som föreskrivs i 29 § till en myndighet eller en sammanslutning som tillsatts för att sköta ett offentligt uppdrag lämna ut uppgifter som är nödvändiga för fullgörandet av ett enskilt uppdrag, om det är uppenbart att utlämnandet av uppgiften inte orsakar väsentlig olägenhet för de intressen för vilkas skyddande sekretess har föreskrivits.

Utöver ovannämnda bestämmelser ingår bestämmelser om utlämnande av information också i 92 § och 93 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Enligt lagens 92 § har de tjänstemän som förebygger och avslöjar brott inom försvarsmakten rätt att av en myndighet samt av en sammanslutning och person som har anförtrotts en offentlig uppgift, avgiftsfritt och trots sekretessbestämmelserna få de uppgifter och handlingar som behövs för att ett uppdrag enligt 86 § 1 mom. ska kunna utföras, om inte lämnande av sådana uppgifter eller handlingar till huvudstaben eller användningen av uppgifterna som bevis har förbjudits eller begränsats i lag. Dessutom föreskrivs i lagens 93 § om rätt att få uppgifter av en privatperson. De tjänstemän som förebygger och avslöjar brott inom försvarsmakten har rätt att av ett teleföretag och en sammanslutningsabonnent få kontaktuppgifter om en sådan teleanslutning som inte nämns i en offentlig katalog, eller uppgifter som specificerar en teleanslutning, en e-postadress, en annan teleadress eller teleterminalutrustning, om uppgifterna behövs i ett enskilt fall för att ett uppdrag enligt 86 § 1 mom. ska kunna utföras. Försvarsmakten har också med stöd av det

som ovan anförts en omfattande allmän rätt att få information för att sköta sina uppgifter. Den kan begränsas genom uttryckliga bestämmelser om detta. Liksom när det gäller polisen har det ansetts att det i lagen om elektronisk kommunikation ingår en sådan uttrycklig begränsning i fråga om innehållet i meddelanden och förmedlingsuppgifter.

### 2.2.4 Personuppgifter och tillämplig dataskyddslagstiftning

Eftersom den information som utbyts delvis till sin karaktär också kan vara personuppgifter är det nödvändigt att bedöma också den dataskyddslagstiftning som gäller för olika myndigheter, Utgångspunkten är att på myndigheternas verksamhet tillämpas allmänna dataskyddsförordningen (EU) 2016/679 och den nationella lagstiftning som kompletterar den, såsom dataskyddslagen (1050/2018). Det bör dock beaktas att i polisens verksamhet utom den allmänna dataskyddsförordningen också tillämpas lagen om behandling av personuppgifter i brottmål vid förebyggande, avslöjande och utredning samt förande till åtalsprövning av vissa brott. Lagen om behandling av personuppgifter i polisens verksamhet tillämpas vid genomförande av grundläggande uppgifter som avses i 1 kap. 1 § i polislagen, om inte annat föreskrivs annanstans i lag.

Dessutom tillämpas lagen om behandling av personuppgifter i brottmål på Försvarsmakten till den del som det är fråga om övervakning av landområde, vattenområde och luftrummet samt för tryggande av territoriell integritet samt handräckning för tryggande av allmän ordning och säkerhet, förhindrande och avbrytande av terrorism samt annat tryggande av samhället. Lagen om behandling av personuppgifter i brottmål tillämpas på Försvarsmakten också vid förebyggande, avslöjande och utredning av brottmål. För detta finns en separat lag om behandling av personuppgifter inom Försvarsmakten, som tillämpas vid sidan av lagen om behandling av personuppgifter i brottmål med några undantag.

Utöver ovannämnda bestämmelser kan också Europaparlamentets och rådets direktiv om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (2002/58/EG), dvs. dataskyddsdirektivet för elektronisk kommunikation, tillämpas. Direktivet har satts i kraft genom lagen om tjänster inom elektronisk kommunikation. Bestämmelserna tillämpas i synnerhet på förmedlingsuppgifter.

### 2.2.5 Utvärdering av lagstiftningen om myndigheternas informationsutbyte

De myndigheter som lagförslaget gäller har i sin verksamhet omfattande rättigheter att få information. Utbytet av information mellan myndigheterna begränsas i praktiken av begränsande bestämmelser som tryggar konfidentialiteten i kommunikation och å andra sidan brandmursbestämmelserna mellan brottsbekämpning och underrättelseverksamhet, Begränsningarna gällande samarbetet mellan myndigheterna finns alltså av grundade orsaker som är förknippade med skyddet av grundläggande rättigheter enligt grundlagen. I praktiken kan exempelvis polisen och försvarsmakten vid behov ha åtkomst också till de uppgifter som Transport- och kommunikationsverket har tillgång till på grund av sina lagstadgade uppgifter, men I situationer som utvecklas snabbt kan detta göra det svårare att förhindra kränkningar av informationssäkerheten eftersom dessa situationer kan gå snabbt förbi. I normala situationer är de begränsningar som gäller informationsutbytet från grundlagsrättsligt perspektiv fortfarande befogade.

## 2.3 Lagstiftning om handräckning

Med handräckning avses myndigheters verksamhet, där den myndighet som ger handräckning ger handräckning med stöd av lagstiftning som möjliggör handräckning till den myndighet som begär handräckning för att sköta sina lagstadgade uppgifter. Utgångspunkten är att varje myndighet själv ska upprätthålla tillräcklig förmåga för att sköta de uppgifter som åligger den med

stöd av lagen. Vid handräckning är det fråga om att en myndighets befogenheter används för att assistera en annan myndighet med att sköta de uppgifter som ankommer på den enligt lag på ett sätt som inte är möjligt för den myndighet som begär handräckning exempelvis för att den inte har befogenhet att agera i en specialsituation eller saknar förmåga.

Befogenhet att ge handräckning och rätt att få handräckning baserar sig på specialbestämmelser. De centrala bestämmelserna om handräckning vid utredning och förebyggande av kränkningar av informationssäkerheten finns i lagen om tjänster inom elektronisk kommunikation, i polislagen och lagen om Försvarsmakten. Dessutom finns bestämmelser om handräckning i TUVE-lagen. Utöver specialbestämmelserna om givande av handräckning finns i förvaltningslagen bestämmelser om myndigheternas allmänna skyldighet att samarbeta.

Med stöd av 10 § i förvaltningslagen ska varje myndighet inom ramen för sin behörighet och i den omfattning ärendet kräver på andra myndigheters begäran bistå dessa i skötsel av en förvaltningsuppgift, och även i övrigt sträva efter att främja samarbetet mellan myndigheterna, Det samarbete som avses i förvaltningslagen betyder dock inte handräckning, om vilken föreskrivs särskilt.

I förarbetena till förvaltningslagen (RP 72/2002 rd) görs en skillnad mellan att ge hjälp och ge handräckning så att med hjälp avses närmast att ge utlåtanden och utredningar som behövs för att utreda och avgöra ett förvaltningsärende till den myndighet som begär det. Bestämmelsen förutsätter inte i sig att samarbetet ska basera sig på behandlingen av ett ärende som år under behandling utan det kan också vara fråga om bistånd innan ärendet tas upp till behandling eller efter att ärendet avgjorts. Innehållet i samarbetet mellan myndigheter borde tolkas brett så att det kan omfatta olika former av samarbete från skriftligt förfarande till olika slag av förhandlingar. Med handräckning avses däremot enligt förarbetena vanligen att en myndighet bistår en annan myndighet vid skötseln av en uppgift som hör till den faktiska förvaltningsverksamheten eller till faktisk myndighetsutövning, såsom ovan beskrivits. I förarbetena till förvaltningslagen konstateras dessutom att man av samarbetsskyldigheten inte kan härleda någon allmän skyldighet att ge information utan att myndigheterna agerar för att fullgöra uppgifter inom sin egen förvaltningssektor, inom sina egna befogenheter och inom gränserna för sin egen tystnadsplikt.

Om Transport- och kommunikationsverkets rätt att få och möjlighet att ge handräckning föreskrivs i 309 § i lagen om tjänster inom elektronisk kommunikation. Transport- och kommunikationsverket har enligt lagens 309 § 1 mom. rätt att få handräckning av polisen, Tullen och Gränsbevakningsväsendet för tillsynen över efterlevnaden av och för verkställigheten av denna lag samt bestämmelser som utfärdats och föreskrifter som meddelats med stöd av den, samt rätt att av försvarsmakten få handräckning för att utreda orsakerna till störningar i radiokommunikationen. Dessa bestämmelser om handräckning har åtminstone inte till fullo ansetts möjliggöra begäran om handräckning i cyberstörningssituationer. Med stöd av 309 § 2 mom. i lagen kan Transport- och kommunikationsverket på begäran ge andra myndigheter experthjälp som handräckning. Beslut om att lämna handräckning fattas av kommunikationsministeriet. Med stöd av 309 § 3 mom. berättigar inte lämnande av handräckning Transport- och kommunikationsverket att till andra myndigheter lämna ut information om meddelanden, förmedlingsuppgifter eller lokaliseringsuppgifter eller om konfidentiella radiosändningars innehåll och existens.

I 1 § i 9 kap. i polislagen finns bestämmelser om handräckning som ges av polisen. Polisen ska på begäran ge andra myndigheter handräckning, om så föreskrivs särskilt. Polisen ska ge andra myndigheter handräckning också för fullgörande av en lagstadgad tillsynsskyldighet, om den myndighet som begär handräckning hindras i sin tjänsteutövning. En polisman som hör till befälet ska fatta beslut om givande av handräckning om inte något annat föreskrivs i lag.

I 2 § i 9 kap. i polislagen finns bestämmelser om handräckning som ges till polisen. En myndighet ska inom ramen för sin behörighet ge polisen sådan handräckning som denna behöver för sina uppdrag. Beslut om att begära handräckning ska fattas av en polisman som hör till befälet, om inte något annat föreskrivs särskilt eller om inte sakens brådskande natur föranleder något annat. Om försvarsmaktens handräckning till polisen föreskrivs separat i lagen om försvarsmaktens handräckning till polisen, som behandlas senare.

Med stöd av 2 § 1 mom. 2 punkten i lagen om försvarsmakten hör till Försvarsmaktens uppgifter stödjande av andra myndigheter, vilket innefattar bland annat handräckning för upprätthållande av allmän ordning och säkerhet, för förhindrande och avbrytande av terroristbrott och andra brott som orsakar allvarlig fara för människors liv eller hälsa samt för skyddande av samhället i övrigt. Enligt 11 § i samma lag kan Försvarsmakten ge handräckning för skyddande av samhället enligt vad som föreskrivs i lagen om bekämpning av oljeskador (1673/2009) eller i någon annan lag.

Försvarsmakten kan ge handräckning också för annat skyddande av samhället med stöd av 11 §. Enligt detaljmotiveringen i lagens förarbeten avses med detta att Försvarsmakten kan ge handräckning då tryggandet av samhället förutsätter sådan personal, sådant material och kunnande som Försvarsmakten har. Försvarsmakten kan som organisation ge handräckning för en uppgift som inte hör till Försvarsmaktens övriga uppgifter. Detta kräver dock att det finns bestämmelser om handräckningen också i den lagstiftning som gäller mottagaren av handräckningen. Således kunde exempelvis Cybersäkerhetscentret vid Transport- och kommunikationsverket i dagens läge ge handräckning till Försvarsmakten i form av experthjälp med stöd av 309 § i lagen om elektroniska tjänster, medan åter Försvarsmakten inte kan ge Transport- och kommunikationsverket handräckning för annat än utredning av orsakerna till störningar i radiokommunikation. Å andra sidan har det i lagen om försvarsmakten inte särskilt föreskrivits om Försvarsmaktens rätt att få handräckning.

Om Försvarsmaktens handräckning till polisen föreskrivs i lagen om Försvarsmaktens handräckning till polisen (342/2022, handräckningslagen). Enligt lagens 2 § har polisen rätt att få handräckning av Försvarsmakten endast om handräckning på grund av polisens otillräckliga resurser behövs för utförandet av en uppgift som enligt lag ankommer på polisen och handräckningen kan ges utan att äventyra Försvarsmaktens uppgifter enligt 2 § 1 mom. 1 punkten i lagen om försvarsmakten. Enligt 12 § i handräckningslagen svarar polisen för den allmänna ledning av situationen som behövs för ett tryggt utförande av handräckningsuppdraget samt för samordningen av polisens och Försvarsmaktens funktioner.

I 90 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten föreskrivs om assistans av polisen och samverkan med polisen vid förebyggande och avslöjande av brott. Det är inte fråga om egentlig handräckning utan om assistans till myndigheterna. Enligt bestämmelsen kan polisen om de som förebygger och avslöjar brott inom försvarsmakten inte har behörighet att utföra en åtgärd som behövs för skötseln av ett uppdrag enligt 86 § 1 mom., utföra en sådan enskild åtgärd som polisen har behörighet till. Detta kan gälla antingen utövande av enskilda befogenheter eller att man tillsammans genomför hela den ifrågavarande uppgiftshelheten.

### 2.4 EU-lagstiftning och unionens domstolspraxis

Enligt artikel 346 i fördraget om Europeiska unionens funktionssätt ligger de åtgärder som gäller den nationella säkerheten utanför unionens behörighet, och om dem bör således lagstiftas nationellt. Av denna orsak ingår i unionens lagstiftning ofta undantag som gäller den nationella säkerheten. Till förslaget ansluter sig dock också EU-lagstiftning som behöver beaktas.

### 2.4.1 NIS-direktivet

Om betydande kränkningar av informationssäkerheten har utfärdats Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, dvs. det så kallade NIS-direktivet. I direktivet föreskrivs bland annat om säkerhets- och informationskrav på leverantörer av centrala tjänster och leverantörer av digitala tjänster. I bilaga II till NIS-direktivet har identifierats de sektorer och delområden inom sektorer som anses vara centrala leverantörer av tjänster i situationer med kränkningar av informationssäkerheten. Dessa aktörer har med tanke på direktivet ansetts vara sådana som tillhandahåller tjänster som är viktiga för att upprätthålla kritisk samhällelig och/eller ekonomisk verksamhet, tillhandahåller tjänster som är beroende av nätverks- och informationssystem eller om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

Enligt direktivet ska de behöriga myndigheterna för de olika sektorerna samarbeta med enheter som reagerar på och utreder kränkningar av informationssäkerheten (CSIRT). I Finland är CSIRT-aktören Transport- och kommunikationsverkets Cybersäkerhetscenter. och behöriga myndigheter är Energiverket, Finansinspektionen, Valvira, NTM-centralen, jord- och skogsbruksministeriet samt Transport- och kommunikationsverket. På leverantörer av kritiska tjänster och digitala tjänster ställs säkerhetskrav och betydande informationssäkerhetsstörningar ska anmälas utan onödiga dröjsmål till den behöriga myndigheten. Vid bedömningen av hur betydande störningen är bör beaktas det antal som påverkas av störningen i tjänsten, hur länge störningen räcker samt hur stort geografiskt område störningen påverkar.

EU-rådet och parlamentet har i maj 2022 nått preliminärt samförstånd om ett nytt cybersäkerhetsdirektiv (NIS2-direktivet), som kommer att ersätta det gällande NIS-direktivet.

### 2.4.2 Direktivet om integritet och elektronisk kommunikation

I direktivet om integritet och elektronisk kommunikation (2002/58/EY, ePrivacy-direktivet) föreskrivs om behandling av personuppgifter och integritetsskydd inom elektronisk kommunikation. Enligt direktivet är kommunikation som sker genom tjänster för elektronisk kommunikation och trafikuppgifterna i samband med den konfidentiella. Det ska särskilt förbjudas att andra personer utan användarens samtycke avlyssnar, uppfångat med tekniskt hjälpmedel, lagrar eller med andra metoder fångar upp eller övervakar kommunikationen och därmed förbundna uppgifter, utom när de har laglig rätt att göra detta i enlighet med artikel 15.1. Enligt denna punkt får medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i direktivet när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv 95/46/EG.

I rättspraxis gällande unionens domstols tolkning av ePrivacy-direktivet har kommunikationens konfidentialitet betonats som en del av respekten för privatlivet enligt artikel 7 samt skyddet av privatlivet enligt artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Enligt rättspraxis kan man endast med mål som gäller bekämpning av allvarlig brottslighet eller förebyggande av allvarliga hot mot den allmänna säkerheten motivera att myndigheterna med stöd av den nationella lagstiftningen ges rätt till sådana trafik- eller lokaliseringsuppgifter, som utgör en helhet som kan göra det möjligt att dra detaljerade slutsatser om privatlivet i fråga om en användare av elektronisk kommunikation. Dessutom begränsas en behörig myndighets rätt att få information till det som är absolut nödvändigt (dom 5.4.2022 Comissioner of an Garda

Síochána m.fl  C-140/20 110 punkten dom 21.12.2016, Tele2 Sverige och Watson m.fl., C-203/15 och C-698/15, EU: C:2016:970, 99 och 118 punkten, dom 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 54 punkten, dom 2.3.2021, Prokuratuur, C-746/18, EU:C:2021:152, 35 punkten). För att säkerställa de ovannämnda förutsättningarna har det ansetts vara väsentligt att myndigheternas rätt att få information förutsätter ett oberoende förvaltnings-organs, såsom en domstols, förhandsövervakning. (dom 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, EU:C:2020:791, 189 punkten och Prokuratuur, 51 punkten).

### 2.4.3 Allmänna dataskyddsförordningen

I EU:s allmänna dataskyddsförordning (EU) 2016/679 (nedan dataskyddsförordningen) föreskrivs om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter. Förordningen tillämpas på behandling av personuppgifter, som är delvis eller helt automatisk samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Territoriellt tilllämpas förordningen på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller en personuppgiftshandläggare som är etablerad i unionen. Dessutom tillämpas förordningen på behandling av personuppgifter som avser registrerade som befinner sig i unionen även om den personuppgiftsansvarige eller personuppgiftshandläggaren inte är etablerad i unionen, om behandlingen har anknytning till övervakning av registrerades beteende så länge beteendet sker inom unionen. Utbyte av uppgifter, som anses vara personuppgifter, mellan myndigheter anses således i princip höra till förordningens tillämpningsområde.

Enligt artikel 5 i förordningen ska personuppgifter behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade och de ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och de får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (ändamålsbegränsning). Behandlingen är enligt artikel 6 i förordningen laglig bland annat om den är nödvändig för att fullgöra en rättslig förpliktelse som åligger den personuppgiftsansvarige eller för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.  Dessutom uppfylls laglighetskravet om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Då behandlingen sker för att utföra en uppgift av allmänt intresse ska grunden för behandlingen föreskrivas antingen i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

Väsentligt när det gäller informationsutbytet mellan myndigheter i situationer med allvar-liga kränkningar av informationssäkerheten är att uppgifter behandlas för något annat ändamål än det ursprungliga. Enligt artikel 6.4 ska om en behandling sker för andra ändamål än det ändamål för vilket personuppgifterna samlades in för det första beaktas de mål som avses i artikel 23.1 och dessutom beaktas att behandling som sker för ett annat ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in. Omständigheter som ska beaktas är kopplingarna mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen. det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige, om särskilda kategorier av personuppgifter behandlas eller huruvida personuppgifter om fällande domar i brottmål och överträdelser behandlas, eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen och lämpliga skyddsåtgärder.

Enligt artikel 23.1 i förordningen är det möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftshandläggaren omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i förordningen, såsom den ändamålsbegränsning och tillämpningsområdet för de

rättigheter och skyldigheter som avses i artikel 5, om en sådan begränsning sker med respekt för de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa bland annat den nationella säkerheten, försvaret, den allmänna säkerheten eller förebyggande, utredning eller avslöjande av brott. I punkt 2 i artikeln uppräknas omständigheter som vid behov bör beaktas vid ovannämnda lagstiftningsåtgärder.

### 2.4.4 Dataskyddsdirektivet för brottsbekämpning

Utom den allmänna dataskyddsförordningen bör med tanke på propositionen beaktas Europaparlamentets och rådets direktiv om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EU) 2016/680. dvs. dataskyddsdirektivet för brottsbekämpning. Direktivet och den allmänna dataskyddsförordningen utgör tillsammans det så kallade dataskyddspaketet, som består av EU:s gällande dataskyddslagstiftning tillsammans med ePrivacy-direktivet. Dataskyddsdirektivet för brottsbekämpning har nationellt satts i kraft genom lagen om be-handling av personuppgifter i brottmål.

Syftet med dataskyddsdirektivet för brottsbekämpning är att säkerställa skyddet av personuppgifter inom direktivets tillämpningsområde samt underlätta uppgifternas fria rörlighet mellan medlemsstaternas polis- och rättsmyndigheter. I dataskyddsdirektivet för brottsbekämpning ingår utom allmänna bestämmelser också bestämmelser om allmänna principer, registeransvariga, handläggare av personuppgifter, överföring av personuppgifter till tredje land eller till internationella organisationer, tillsynsmyndigheter, samarbete, rättsskyddsmetoder, ansvar samt påföljder.

## 2.5 Bedömning av nuläget

För myndigheternas samarbete vid kränkningar av informationssäkerheten finns i sedvanliga situationer mycket väl etablerade förfaranden och i regel uppfattar myndigheterna att samarbetet i flera avseenden fungerar rätt bra. Såsom ovan konstaterats i samband med utvärderingen av myndigheternas uppgifter är myndigheternas uppgifter i någon mån överlappande särskilt när det gäller utredning av kränkningar av informationssäkerheten och på skötseln av dem tillämpas liknande metoder oberoende av vilken myndighet det är fråga om, men syftet och ändamålet med utredningen varierar. Också när det gäller lägesbilden och producerandet av lägesuppgifter finns delvis motsvarande överlappning.

Det finns inga allvarliga brister när det gäller lagstiftningen om myndigheternas informationsutbyte i normala situationer. Det finns vissa begränsningar som är ändamålsenliga med tanke på skyddet av innehållet i konfidentiella meddelanden gällande Transport-.och kommunikationsverkets rätt att utlämna information om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter samt innehållet i och existensen av konfidentiella radiosändningar särskilt till polisen eller Försvarsmakten i de fall då inga informations-säkerhetskränkningar eller hot om kränkningar direkt riktas till dem. En annan faktor som begränsar Försvarsmaktens och polisens interna informationsutbyte är den så kallade brandmurslagstiftningen mellan brottsbekämpning och underrättelseverksamhet. Också denna lagstiftning är motiverad från grundlagsrättsliga utgångspunkter som gäller rättskydd och också skydd av kommunikationens konfidentialitet i verksamhet i informationsnätsmiljö. Den nuvarande lagstiftningen medför dock i någon mån utmaningar när det gäller uppgörandet av lägesbilden på teknisk nivå också under normala förhållanden, eftersom förmedlingsuppgifter är sekretessbelagda. Å andra sidan anses den gällande

lagstiftningen inte fungera på bästa möjliga sätt i situationer som förutsätter att myndigheterna reagerar snabbt och i samarbete i allvarliga fall av kränkning av informationssäkerheten.

Utlämnandet av information är således delvis reglerad, men det har angetts trösklar och ändamål på olika nivåer för utlämnande av information, vilket medför olägenheter i praktiska situationer särskild då regleringen inte är kongruent, konsekvent eller heltäckande. Det kan vara oklart i vilken utsträckning de aktuella uppgifterna kan utlämnas, i synnerhet om båda parter i och för sig kan ha rätt att behandla dessa uppgifter.

De nuvarande bestämmelserna om utbyte av information har också i någon mån en dubbel uppbyggnad så att det föreskrivs separat om myndigheternas rätt att få vissa uppgifter och å andra sidan om myndigheternas rätt att lämna ut uppgifter. En sådan lagstiftning är enligt grundlagsutskottets synvinkel ägnad att medföra tolkningsproblem, även om den inte egentligen är konstitutionellt problematisk (GrUU 71/2014 rd, s. 3).

Oklarhet i tolkningen har förorsakats av de frågor som gäller utlämnande av personuppgifter. En del av de uppgifter som utbyts mellan myndigheterna, särskilt uppgifter på mera teknisk nivå, såsom förmedlingsuppgifter, anses vara personuppgifter, eftersom man med stöd av dem under vissa förutsättningar kan identifiera en person. I sådana situationer har det i viss mån blivit oklart hur sådana uppgifter mellan myndigheterna kan lämnas ut med stöd av allmänna bestämmelser om utlämnande av information, i synnerhet om informationen används också för andra ändamål än den ursprungliga, i den betydelse som avses i den allmänna dataskyddsförordningen, vilket enligt dataskyddsförordningen förutsätter att utlämnandet av informationen är stadgad i lag. En del av polisens och Försvarsmaktens uppgifter omfattas också av lagstiftningen om behandling av personuppgifter i brottmål. Dessutom har polisen och Försvarsmakten sina egna personuppgiftslagar, vilka kompletterar både den allmänna dataskyddsförordningen och lagen om behandling av personuppgifter i brottmål, vilket är ägnat att göra det oklart vilken personuppgiftslagstiftning som ska tillämpas. Dessutom används vid utredning av kränkningar av informationssäkerheten ofta IP-adresser för att utreda källorna till kränkningen. Den tolkning enligt vilket IP-adresser i princip tolkas som personuppgifter är dock i vissa fall problematisk eftersom alla IP-adresser inte används av enskilda personer utan det kan vara fråga om bland annat nätanläggningars IP-adresser eller IP-adresser som används av webbsidor och det då inte är fråga om personuppgifter. Personuppgiftsfrågan hänger också delvis samman med att det också finns rum för tolkning när det gäller begreppet förmedlingsuppgifter.

I fråga om bestämmelserna om handräckning har särskilt förfarandena mellan polisen och Försvarsmakten etablerats i samband med traditionell fysisk verksamhet. När det gäller cyberverksamhetsmiljön har situationen inte ännu etablerats på motsvarande sätt. Dessutom bör beaktas att det för försvarsmakten inte i lagen om Försvarsmakten har föreskrivits om någon rätt att ta emot handräckning av en annan myndighet. Också av Cybersäkerhetscentret vid Transport- och kommunikationsverket begärs handräckning i form av experthjälp för stöd av utförandet av andra myndigheters uppgifter. Transport- och kommunikationsverkets möjlighet att ge handräckning är inskriven i lagstiftningen på allmän nivå och den kan inte anses medföra begränsningar för begäran om handräckning. Däremot finns det brister när det gäller Transport- och kommunikationsverkets möjlighet att få handräckning exempelvis för att utreda allvarliga kränkningar av informationssäkerheten, där verkets egna resurser skulle ta slut. Sådana färdigheter har i Finland utom Transport- och kommunikationsverket för närvarande polisen, skyddspolisen och Försvarsmakten. I framtiden borde verkets rätt att begära handräckning av dessa myndigheter utvidgas när det gäller kränkningar av informationssäkerheten.

Det har funnits oklarhet i fråga om tolkningen av kommunikationsförmedlares rätt att på eget initiativ lämna ut information till Transport- och kommunikationsverket om meddelanden och

förmedlingsuppgifter vid kränkningar av informationssäkerheten. För teleföretagens del finns anmälningsskyldighet vid betydande kränkningar av informationssäkerheten, men på mindre kränkningar kan detta inte tillämpas, även om det med den information som fås av dem eventuellt också skulle vara möjligt att förhindra kränkningar av informationssäkerheten. Bestämmelserna gäller dessutom endast teleföretag även om också andra aktörer förmedlar kommunikation och det skulle vara ändamålsenligt att för dem göra det möjligt att lämna ut information för att förhindra kränkningar av informationssäkerheten.

Enskilda observationer som ingår i den nuvarande lagstiftningen gäller också beslutsprocesserna i samband med Transport- och kommunikationsverkets verksamhet, såsom uppgörandet av begäran om handräckning och utlämnande av uppgifter om kränkningar av informationssäkerheten till myndigheter i andra länder som ansvarar för informationssäkerheten. Förfarandena borde kunna göras lättare så att det i stället för kommunikationsministeriet är verket självt som beslutar om dessa åtgärder.

Utom de begränsningar som lagstiftningen ställer kan det också i någon mån finnas utmaningar när det gäller nivån på personalens kunskap.om vilka uppgifter som kan lämnas ut och på vilka grunder. Särskild vikt bör fästas vid dessa frågor inom personalens utbildning.

Det finns också större frågor i samband med nuläget, till exempel när det gäller myndigheternas befogenheter och skyldigheter, vilka inte utvärderas närmare inom ramen för detta projekt. Dessa kommer dock att utvärderas i ett mera omfattande utredningsprojekt som inletts av inrikesministeriet och försvarsministeriet, där myndigheternas verksamhetsförutsättningar för säkerställandet av den nationella cybersäkerheten, bekämpningen av cyberbrottsligheten och cyberförsvaret utvärderas.

## 3 Målsättning

Propositionens målsättning är att förbättra tryggheten i samhället och uppfyllandet av de grundläggande rättigheterna, särskilt skyddet av konfidentiell kommunikation, genom att förbättra myndigheternas verksamhetsförutsättningar vid utredningen av sådana kränkningar av informationssäkerheten vilkas skadliga verkningar i allvarliga situationer i stor utsträckning kan drabba funktioner som är centrala för samhällets verksamhet. Målsättningen med regeringens proposition är att förbättra myndigheternas samarbete genom att utveckla lagstiftningen om handräckning och informationsutbytet vid utredning av sådana kränkningar av informationssäkerheten som är betydande och har allvarliga konsekvenser och vid hot om sådana kränkningar och vid elimineringen av dessa konsekvenser.

Propositionens målsättning är att skapa tydliga förutsättningar för myndigheternas informationsutbyte vid allvarliga kränkningar av informationssäkerheten genom att föreskriva om inbördes rättigheter att utbyta nödvändig information för de myndigheter som är centrala vid utredning av kränkningar. Dessutom är målet att skapa förutsättningar för behövlig handräckning mellan myndigheterna så att lagstiftningen inte utgör något hinder för begäran om handräckning. I fråga om Transport- och kommunikationsverket är målet också att göra beslutsprocesserna i handräckningsförfarandet lättare.

## 4 Förslagen och deras konsekvenser

### 4.1 De viktigaste förslagen

Det viktigaste förslaget i propositionen gäller myndigheternas inbördes informationsutbyte vid betydande kränkningar av informationssäkerheten eller vid allvarliga hot om sådana, där verkningarna omfattar samhällets vitala funktioner. Förslaget är en ny bestämmelse om informationsutbyte i enskilda fall, som tillämpas i ovannämnda allvarliga situationer. Det är ändamålsenligt att lagstiftningen bygger på bestämmelser som gäller enskilda fall som avviker från informationsutbytet i normala situationer, eftersom begräsningarna av informationsutbytet i normala situationer är motiverade särskilt på grund av att särskilt skyddet av konfidentiella meddelanden omfattas av skyddet av grundläggande rättigheter.

Det föreslås att lagstiftningen om handräckning kompletteras när det gäller handräckning som Transport- och kommunikationsverket får från sådana myndigheter som i praktiken har förmåga att utreda kräkningar av informationssäkerheten eller hot om sådana kräkningar. Till dessa myndigheter hör polisen, skyddspolisen och Försvarsmakten. Även om handräckning i viss mån uppfattas som ett tungt förfarande vid sidan av annat myndighetssamarbete är det dock nödvändigt att föreskriva om detta för undantagssituationer, så att inte lagstiftningen blir ett hinder för att en myndighet som behöver handräckning ska kunna sköta sin uppgift.

Det föreslås att behandlingen av begäran om handräckning vid Transport- och kommunikationsverket görs lättare, så att verket självt i framtiden beslutar om lämnandet av handräckning i ställer för kommunikationsministeriet. Motsvarande ändring i beslutsprocessen föreslås också i fråga om utlämnandet av information till en sådan i en annan stat verksam myndighet eller annan motsvarande aktör som har till uppgift att förebygga eller utreda kränkningar av informationssäkerheten som är riktade mot kommunikationsnät och kommunikationstjänster. Dessutom får uppgifter i fortsättningen lämnas ut också till sådana organ inom Europeiska unionen eller Nordatlantiska fördragsorganisationen NATO som utreder kränkningar av informationssäkerheten.

I propositionen föreslås också att till lagen fogas en ny bestämmelse om kommunikationsförmedlares rätt att frivilligt lämna ut information till Transport- och kommunikationsverket om förmedlingsuppgifter eller elektroniska meddelanden som förmedlaren behandlar om det behövs för att utreda eller förebygga kränkningar av eller hot mot informationssäkerheten.

Det föreslås att lagen om behandling av personuppgifter i polisens verksamhet och lagen om behandling av personuppgifter inom Försvarsmakten preciseras närmast genom förtydligande bestämmelser om rätt att till Transport- och kommunikationsverket lämna ut personuppgifter som är nödvändiga för skötseln av vissa av verkets uppgifter som gäller kränkningar av informationssäkerheten. Bestämmelser har dock inte någon stor betydelse i praktiska situationer utan det är fråga om harmonisering och förtydligande av lagstiftningen för att undvika olika tolkningsmöjligheter.

### 4.2 De huvudsakliga konsekvenserna

#### 4.2.1 Konsekvenser för myndigheternas verksamhet

Propositionens centrala direkta konsekvenser gäller myndigheternas inbördes förhållanden, förfaringssätt samt administrativa förfaranden vid betydande kränkningar av informationssäkerheten och hot om sådana. Helhetsinverkan på myndigheternas verksamhet bedöms vara liten, eftersom de föreslagna bestämmelserna om informationsutbyte mellan myndigheterna torde komma att tillämpas endast i undantagssituationer, ifall inte antalet sådana situationer ökar

märkbart. I propositionen föreslås att möjligheterna till samarbete mellan myndigheterna förbättras genom att informationsutbytet effektiveras. Förslaget kan anses underlätta och förtydliga växelverkan mellan myndigheterna och försnabba verksamheten i dessa situationer. En tydlig rätt till informationsutbyte mellan myndigheterna försnabbar myndigheternas möjligheter att reagera på betydande kränkningar av informationssäkerheten.

Under beredningen genomfördes en övning i informationsutbyte mellan myndigheterna enligt förslaget, där det utvärderas hur väl förslaget kan tillämpas i praktiken. Som ett resultat av övningen konstaterades att det i praktiken kan visa sig vara svårt att bedöma om tröskelvärdet för utbyte av information överskrids, i synnerhet som helhetsbilden av kränkningen av informationssäkerheten och av hur betydande den är ofta kan bildas först genom utbyte av uppgifter. Dessa kan dock inte utbytas innan förutsättningarna bedömts, vilket baserar sig på en kombination av uppgifter. Detta kan medföra utmaningar med tanke på tillämpningen av förslaget.

Förslaget påverkar inte direkt myndigheternas uppgifter sådana som de nu är enligt lagstiftningen. En ändring som i någon mån påverkar myndigheternas uppgifter ansluter sig till handräckning som lämnas av Försvarsmakten, polisen och skyddspolisen till Transport- och kommunikationsverket. För polisen och Försvarsmakten är denna uppgift endast i någon mån ny, eftersom verket har kunnat få handräckning av dessa myndigheter också hittills. I praktiken har inte Transport- och kommunikationsverket begärt handräckning av andra myndigheter i samband med kränkningar av informationssäkerheten. Konsekvenserna kommer antagligen därför att bli rätt små. Avsikten är att det normala samarbetet mellan myndigheterna ska fortsätta på samma sätt som hittills.

Det kan antas att utnyttjandet av specialkunnande från ett vidare myndighetsfält förbättrar hanteringen och analysen av kränkningar av informationssäkerheten och hot om sådana, vilket å andra sidan ger den aktör som är föremål för kränkningen bättre förutsättningar att skaffa de tjänster som behövs för att rätta till situationen. När det gäller informationssäkerheten är också personalens kompetens viktig, vilket framförallt i vissa speciella situationer som kräver tekniskt kunnande kan finnas endast hos några personer i Finland eller t.o.m. i hela världen.

I förslaget ingår två ändringar som gäller beslutsprocesserna, vilkas syfte är att lätta på det administrativa förfarandet i Transport- och kommunikationsverket. Förslagen om underlättande av det administrativa förfarandet gäller att kommunikationsministeriet inte längre ska besluta om handräckning som ges av Transport- och kommunikationsverket eller om information som verket lämnar ut till utländska myndigheter som är behöriga att utreda kränkningar av informationssäkerheten.

Förslaget syftar till att vid betydande kränkningar av informationssäkerheten eller hot om sådana trygga bland annat de funktioner som påverkar den offentliga maktens beslutsförmåga och myndigheternas verksamhetsförutsättningar. Förbättrandet av samarbetet mellan myndigheterna vid förebyggandet av att hot uppfylls och å andra sidan kränkningar som redan ägt rum kan antas inverka positivt på den offentliga maktens beslutsförmågan också vid allvarliga kränkningar av informationssäkerheten. Konsekvenserna bedöms vara motsvarande också på annan myndighetsverksamhet.

Förslaget om kommunikationsförmedlares rätt att lämna ut förmedlingsuppgifter och uppgifter om meddelanden till Transport- och kommunikationsverket förbättrar verkets förutsättningar att utreda och förebygga kränkningar av informationssäkerheten samt gör det möjligt att göra upp en mera heltäckande lägesbild. Bestämmelsen påverkar således också den dagliga verksamheten. På basis av en synpunkt som framförts i ett utlåtande är det möjligt att en kommunikationsförmedlares tröskel för att lämna ut information stiger, eftersom myndigheten kanske kan

börja utreda om rätten att behandla uppgifter enligt lagen om elektronisk kommunikation har uppfyllts i fråga om denna uppgift. Detta kan vara en utmaning särskilt för små och medelstora företag.

### 4.2.2 Ekonomiska konsekvenser

Förslaget bedöms ha endast små ekonomiska konsekvenser. Att Transport- och kommunikationsverket får större möjligheter att begära handräckning av polisen, skyddspolisen och Försvarsmakten kan om de används i någon mån medföra kostnader för den offentliga ekonomin, men det skulle också då enligt bedömningen vara fråga om endast mindre kostnader av engångsnatur. Handräckningen skulle vara experthjälp eller utrustningshjälp och kostnaderna begränsar sig då i praktiken till dessa funktioner. Den som begär handräckning svarar för kostnaderna för handräckningen inom ramen för de nuvarande anslagen. Mängden handräckning väntas inte öka i någon betydande grad på grund av förslaget.

### 4.2.3 Konsekvenser för företagen

På bestämmelserna om informationsutbyte enligt förslaget tillämpas vid kränkningar av informationssäkerheten som drabbar funktioner som är centrala för samhällets verksamhet. Många sådana funktioner sköts av privata aktörer. Förbättrande av myndigheternas förmåga att ingripa och samarbetet vid förebyggande, utredning och i någon mån också eliminering av verkningarna begränsar för sin del uppkomsten av menliga kostnader. När det gäller eliminering av verkningarna är den inverkan som myndigheternas verksamhet har på företagen i någon mån begränsad, eftersom det ofta är aktören själv som har ansvaret för dessa. Myndigheterna kan dock stöda företag i sådana situationer. Ett mera omfattande informationsutbyte mellan myndigheterna förbättrar kunskapen om läget, vilket för det lättare för dem att agera bättre också i förhållande till företag som drabbats av intrånget.

Förslaget bedöms ha konsekvenser för företagen närmast i de situationer då en betydande kränkning av informationssäkerheten eller ett allvarligt hot om en sådan drabbar ett företag vars verksamhet är central för samhällets verksamhet. Enligt de synpunkter som framfördes i remissyttrandena kan konsekvenserna variera kraftigt beroende på vilken bransch det är fråga om. Näringslivets centralförbund har konstaterat att konsekvenserna sannolikt skulle vara betydande särskilt för telekommunikations- och finanssektorn samt inom andra kritiska sektorer. Å andra sidan är samarbetet inom dessa sektorer på grund av den omfattande lagstiftning som gäller dessa sektorer redan nu ganska regelbundet och välfungerande.

Vid kränkningar av informationssäkerheten kan myndigheternas förbättrade verksamhetsförutsättningar från företagens perspektiv bedömas vara i huvudsak positiva, och då kan man i bästa fall förhindra att ett hot om kränkning av informationssäkerheten realiseras och myndigheterna kan stöda företagen vid elimineringen av verkningarna av kränkningen av informationssäkerheten. Det är svårt att bedöma de kostnader som orsakas av kränkningar av informationssäkerheten, men utöver det som ovan nämnts kan t.ex. sabotageprogram som används för utpressning orsaka företagen förluster på miljontals euro ifall den lösen som krävs betalas ut eller verksamheten avbryts. Konsekvenserna för företagen av sabotageprogram som förstör data kan vara ännu mer förlamande för verksamheten särskilt om företagets verksamhet till stor del består av informationssystemens verksamhet och data som finns i informationssystemen. Syftet med förslaget är att minska de skadliga verkningarna av kränkningar av informationssäkerheten genom att förbättra myndigheternas förmåga och samarbete så att de kan ingripa i betydande kränkningar av informationssäkerheten som har skadliga verkningar och förebygga hot om sådana.

Helhetskostnaderna för dataskyddsproblem och de funktionsstörningar de orsakar har bedömts bland annat i Förbättring av informationssäkerheten och dataskyddet inom kritiska sektorer i samhället. Arbetsgruppens slutrapport (Kommunikationsministeriets publikation 2021:1, sid 52–54). Om informationssäkerheten och dataskyddet brister inom kritiska sektorer förorsakar det många slag av kostnader, eftersom det utöver kostnaderna på företagsnivå orsakas kostnader för samhället också i större omfattning, exempelvis genom ömsesidigt beroende. De små och medelstora företagens totala kostnader för dataintrång var i USA 2015 cirka 50 000 dollar. Däremot var de totala kostnaderna i stora företag, som sysselsätter mer än 1500 personer, cirka 620 000 dollar. Då man går från konsekvenserna på företagsnivå till störningar i verksamheten i de sektorer som är kritiska på samhällsekonomisk nivå kan kostnadsverkningarna stiga till en storleksklass på tiotals miljoner eller miljarder (Ronikonmäki, Niko-Matti – Sirviö, Tom Henrik: Taloustieteellisiä näkökulmia kyberturvallisuuteen. Kansantaloudellinen aikakausikirja – 117 vsk 2/2021, s. 268). Jämfört med år 2015 har verksamheten dessutom ytterligare utvidgats och blivit mer yrkesmässig och därför kan kostnadsverkningarna nu vara redan betydligt större. Det är överhuvudtaget svårt att få exakt helhetsstatistik över kränkningar av informationssäkerheten eftersom många företag t.ex. för att skydda sitt rykte inte anmäler till myndigheterna om kränkningarna.

Förmedlingsuppgifter och uppgifter om meddelandens innehåll som utlämnas till Transport- och kommunikationsverket omfattas av tystnadsplikt, i vilken nu föreslås ett undantag. Tystnadsplikten har ansetts vara central för skyddet av konfidentiell kommunikation och verksamhet. I den situation som avses i förslaget kan uppgifter som gäller kränkningar av informationssäkerheten eller hot om sådana utlämnas mellan polisen, skyddspolisen, Försvarsmakten och Transport- och kommunikationsverket i större omfattning än tidigare i sådana allvarliga situationer som avses i förslaget, där samhällets säkerhet kan äventyras. Förslaget anger i sig begränsningar när det gäller konfidentialiteten för den information som lämnats ut till myndigheterna och t.ex. uppgifter om offer för kränkningar av informationssäkerheten kan i många fall vara känslig särskilt på grund av risken att den skadar deras rykte. Då man beaktar hur exceptionella sådana situationer är och å andra sidan hur allvarliga de är kan man bedöma att förslaget inte i betydande grad påverkar företagens förtroende för verksamheten vid myndigheternas och särskilt Cybersäkerhetscentret, till vilka frivilliga anmälningar görs. I sig inverkar inte förslaget allmänt på tystnadsplikten när det gäller information, dvs. information som är sekretessbelagd är det också hos den mottagande myndigheten.

#### 4.2.4 Konsekvenser för medborgarnas ställning i samhället

Det kan bedömas att förslagets konsekvenser påverkar också medborgarnas ställning och särskilt skyddet av privatlivet. Kränkningar av informationssäkerheten i sig kan utom på företag ha omfattande verkningar också för vanliga medborgare och hushåll, vilkas upp-gifter exempelvis har varit en del av något större informationssystem, som har drabbats av en kränkning av informationssäkerheten. Då är risken att känsliga uppgifter som finns i systemet läcks ut i offentligheten eller att de missbrukas på något annat sätt. Genom effektivering av myndigheternas verksamhet i allvarliga situationer förbättras möjligheterna att utreda kränkningar av informationssäkerheten. gripa de skyldiga och i bästa fall förebygga dessa, ifall ett allvarligt hot mot informationssäkerheten kan observeras i ett tillräckligt tidigt skede. Förslaget förbättrar indirekt medborgarnas och hushållens ställning genom att förbättra myndigheterna funktionsförmåga när det gäller att ingripa i och utreda sådana betydande kränkningar av informationssäkerheten, vilka kan medföra allvarliga olägenheter för medborgarna och hushållen i samhället.

Förslaget möjliggör för kommunikationsförmedlare en mera omfattande rätt än tidigare att lämna ut förmedlingsuppgifter och uppgifter om meddelandens innehåll till Transport- och

kommunikationsverket. Detta påverkar medborgarnas skydd för privatlivet och skyddet av konfidentiell kommunikation. Meddelandens innehåll är kärnan i kommunikationens konfidentialitet. Ändringens inverkan i detta avseende är om man ser till helheten inte särskilt betydande eftersom Cybersäkerhetscentret också för närvarande har rätt att begära uppgifter om kränkningar av informationssäkerheten och å andra sidan t.ex. meddelanden som innehåller sabotageprogram inte är den mest centrala kärnan i konfidentiell kommunikation. Därför bedöms konsekvenserna i detta avseende som helhet ändå vara små. Som helhet förbättrar ändå förslaget indirekt kommunikationens konfidentialitet genom förebyggande av kränkningar av informationssäkerheten.

### 4.2.5 Konsekvenser för brottsbekämpning och säkerhet

Förslaget bedöms ha konsekvenser som förbättrar den nationella säkerheten och främjar bekämpningen av cyberbrottsligheten, På basis av de erfarenheter man hittills fått av samarbete ingår i informationsutbytet vissa utmaningar, som i de allvarligaste situationerna som kräver snabba åtgärder kan försvara helhetsmässig hantering och observation av situationen mellan myndigheterna. Genom tydligare bestämmelser underlättas myndigheternas samarbete i dessa situationer. Då säkerhetssituationen i samhället förändras måste eventuella allvarliga säkerhetssituationer förutses och syftet med förslaget är att svara på dessa utmaningar.

Eftersom samhällets verksamhet också i nuläget i betydande grad bygger på nätförbindelser och informationssystem och de innehåller också en betydande mängd information om både privatpersoner och sammanslutningar, har deras funktion en kritisk ställning i samhällets verksamhet. Särskilt datatrafikförbindelserna och eldistributionen är funktioner som i stor omfattning påverkar många olika funktioner. Kränkningar av informationssäkerheten som riktas mot elnätens funktion kunde ha mycket betydande verkningar för hela samhället eftersom nästan allt från sjukhus till hushåll fungerar med elektricitet eller t.ex. mot trafikstyrningssystemen. Störningar av data- eller kommunikationsnäts funktion skulle likaså ha omfattande konsekvenser då allt flera funktioner är anslutna till nätet. Många industrisektorer, myndigheternas funktioner, sjuk- och hälsovårdens system bygger ofta på system som är kopplade till nätet. Om dessa systems funktion förhindras skulle de ha betydande skadeverkningar för denna aktörs verksamhet och i värsta fall äventyra samhällets säkerhet också i större omfattning.

Av denna orsak är det viktigt att reagera på kränkningar av informationssäkerheten och minimera konsekvenserna av dem med alla tänkbara metoder, Samarbetet vid allvarliga hot mot informationssäkerheten står i direkt relation till brottsbekämpningen, eftersom eventuella brott ännu kan förhindras i en hotsituation. Det är dock svårt att ta fast brottslingar i cyberbrott t.ex. av den orsaken att det är svårt att spåra brottslingarna, men också därför att cyberbrott går över de statliga gränserna och förövaren därför i praktiken kan finnas var som helst i världen. Klarare bestämmelser underlättar i dessa situationer myndigheternas samarbete. Brottsbekämpningen kan i någon mån underlättas också av bestämmelserna om informationsutbyte i undantagssituationer till den del som de uppgifter som polisen får kan utnyttjas vid utredningen av brottet och påförandet av ansvaret för brottet.

Enligt myndigheternas bedömning förbättrar förslaget om kommunikationsförmedlares frivilliga utlämnande av uppgifter upprätthållandet av den nationella lägesbilden av cybersäkerheten samt utredningen av kränkningar av informationssäkerheten och distributionen av information om dem samt därigenom förebyggandet av kränkningar av informationssäkerheten. Det förbättrar också indirekt informationssäkerheten för kommunikationsnät, tjänster och därmed anslutna informationssystem, vilket bidrar till att trygga också skyddet av privatlivet för användare av kommunikationstjänster.

# 5 Alternativa handlingsvägar

## 5.1 Handlingsalternativen och deras konsekvenser

Som ett alternativ till propositionen har bedömts ett nollalternativ, således att bestämmelserna om informationsutbyte och handräckning lämnas oförändrade. Myndigheterna samarbeta för att utreda, förebygga och eliminera konsekvenserna av kränkningar av informationssäkerheten utgående från nuvarande lagstiftning och inom de uppgifter som ankommer på dem. Myndigheterna kan inbördes utbyta information om kränkningar av informationssäkerheten i enlighet med de villkor som föreskrivits. När det gäller mycket allvarliga kränkningar av informationssäkerheten har det visat sig finnas ett behov kanaler för inbördes informationsutbyte som är snabbare än nu, vilka inte funnits för riktigt alla uppgifter, såsom meddelanden, förmedlingsuppgifter och lokaliseringsuppgifter. Detta har förts fram också i Statsrådets principbeslut om förbättring av datasäkerheten och dataskyddet i samhällets kritiska områden och i slutrapporten från den tidigare arbetsgruppen. Av denna orsak har det ansetts befogat att ändra nuläget i dessa avseenden och lagstiftningen kan därför inte lämnas oförändrad.

Som alternativ lösning har bedömts om situationer med omfattande störningar kunde lösas genom en egen lagstiftning för dem, som skulle byggas upp uttryckligen för allvarliga kränkningar av informationssäkerheten och med tanke på det samarbete som måste göras för att lösa dessa situationer. Under beredningen bedömdes dock att de nuvarande handlingsmodellerna till sina centrala delar upplevts fungera väl och därför finns det inget behov av att på allmän nivå ändra dem ens i allvarliga situationer. Myndigheterna agerar i vilket fall som helst med stöd av sina föreskrivna befogenheter. Dessutom bedömdes att en ny lagstiftning som gäller enskilda situationer skulle vara ägnad att ytterligare komplicera lagstiftningen om informationsutbyte som redan nu är ganska invecklad genom att lägga till ännu ett lager. Det är inte heller i och för sig vanligt att föreskriva om myndigheternas samarbete, utan det skulle också annars vara fråga om en exceptionell handlingsmodell. Genom en lagstiftning av detta slag kunde man i och för sig uppnå motsvarande verkningar som med detta lagförslag, men med tanke på dem som tillämpar lagen kunde en separat lag i praktiken visa sig vara utmanande.

Under beredningen har bedömts olika alternativ för hur man kunde definiera en sådan allvarlig kränkning av informationssäkerheten som har betydande konsekvenser för sektorer som är viktiga för samhällets verksamhet, dvs. i praktiken när undantagsbestämmelser om informationsutbytet borde tillämpas. Utom det alternativ som valts bedömdes som ett alternativ att tillämpa förteckningen i bilagan till NIS-direktivet vid definitionen av samhällets kritiska sektorer, men svårigheten med dem ansågs vara att den är så detaljerad och det då kunde finnas risk för att vissa funktioner faller emellan. En motsats hade varit den allmänt formulerade skrivning, som också varit på remiss, som skulle möjliggöra ett omfattande tillämpningsområde enligt behov, men innehållet i den ansågs vara för opreciserat, och således inte användbart för dem som tillämpar lagen, men också på grund av att de krävs exakta gränser för begränsning av grundläggande rättigheter.

I fråga om skrivning om tröskeln för tillämpning av lagen har olika definitioner bedömts, som ingår t.ex. i 18 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019) eller 244 a § i lagen om tjänster inom elektronisk kommunikation. Förebilden för den förteckning som ingår i lagförslaget är förteckningen i 3 § 6 punkten i beredskapslagen, men inte heller den ansågs direkt lämpa sig för den situation som avses i förslaget.

I samband med beredningen av propositionen har lagstiftningen och myndigheternas uppgifter i Sverige, Norge, Tyskland, Storbritannien och Frankrike bedömts. Bedömningen av dessa sta-

ter beskrivs i avsnitt 5.2. Som ett slutresultat av bedömningen har dock konstaterats att myndigheternas uppgifter och befogenheter varierar så mycket från stat till stat att utländska erfarenheter och utländsk praxis inte direkt har kunnat utnyttjas för att hitta en nationell lösning, utan man måste hitta en lösning för utmaningarna i fråga om de finländska myndigheternas nationella samarbete utgående från den nationella lagstiftningen och de utmaningar den medför för samarbetet.

## 5.2 Lagstiftning och andra handlingsmodeller i utlandet

### 5.2.1 Sverige

#### 5.2.1.1 Behöriga myndigheter

Liksom i Finland har i Sverige grundats en centraliserad myndighet för cybersäkerheten, i vilken samlats uppgifter som betjänar digital säkerhet och cybersäkerhet i hela samhället. Den centrala aktören bland Sveriges cybersäkerhetsmyndigheter är MSB (Myndigheten för samhällsskydd och beredskap) och den avdelning för cybersäkerhet och säkra kommunikationer som verkar under den (Avdelningen för cybersäkerhet och säkra kommunikationer). Till avdelningens ansvarsområde hör bland annat upprätthållandet av CERT-SE (Computer Emergency Response Team) och den fungerar som internationell kontaktpunkt för särskilt samarbetet med EU. Avdelningen följer upp verksamhetsmiljön, tar emot anmälningar från myndigheterna, utvecklar samarbetsformer mellan olika myndigheter och andra aktörer samt tillhandahåller tjänster gällande lägesbilden för cybersäkerheten. MSB har ansvar för åtgärder som gäller civilförsvaret, den allmänna säkerheten och hanteringen av nödsituationer då ingen annan myndighet är ansvarig för dem.

Sveriges nya cybersäkerhetscenter (Nationellt cybersäkerhetscenter) har till uppgift att stärka myndigheternas beredskap att lösa sina egna uppdrag och samtidigt erbjuda bättre möjligheter att öka den nationella förmågan att förebygga, observera och hantera cyberangrepp och andra incidenter på nätet som hotar att skada Sveriges säkerhet. I grundandet av cybersäkerhetscentret har deltagit FRA (Försvarets radioanstalt), Sveriges fösvarsmakt, MSB och Säpo (Säkerhetspolisen). Cybersäkerhetscentret bedriver ett omfattande samarbete med Sveriges post- och telemyndighet (Post- och telestyrelsen), polisen och försvarets materielmyndighet (Försvarets materielverk). Dessa organisationer ges också möjlighet att delta i centrets verksamhet. Cybersäkerhetscentret bedriver ett omfattande samarbete med privata och offentliga aktörer.

I Sverige ska alla statliga verk anmäla om cyberstörningar i verkets informationssystem eller i tjänster som en myndighet tillhandahåller för en annan organisation. Enligt förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (2015:1052) ska en myndighet till MSB skyndsamt rapportera it-incidenter som inträffat i den rapporterande myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som inträffat i tjänster som myndigheten tillhandahåller åt en annan organisation.

För det nationella cyberförsvaret svarar Sveriges försvarsmakt och de verkar som är underställda den. Huvudansvaret har ledningssystemdirektören och cyberförsvarsenheten som är underställda huvudstaben. Cyberförsvaret är dock inte enbart arméns uppgift utan i arbetet deltar tidvis också Säpo och MSB.

På nationell nivå finns flera aktörer inom cybersäkerheten. Huvudsakligen har MSB; Sveriges försvarsmakt, Säpo samt FRA ansvar för cybersäkerheten och dess utveckling. Cybersäkerheten sköts också på flera plattformer för samarbete mellan myndigheterna, av vilka den mest centrala

är SAMFI (Samverkansgruppen för informationssäkerhet). Till medlemmarna i SAMFI hör utom de myndigheter som svarar för handlingsplanen för cybersäkerhetsstrategin också svenska arméns underrättelsetjänst Must (militära underrättelse- och säkerhetstjänsten). NSIT (Nationell samverkan till skydd mot allvarliga IT-hot) verkar som samarbetsorgan för beredskapen för allvarliga hot och hot som riktas mot kritiska verksamheter. Där är Säpo, FRA, Must och Sveriges försvarsmakt representerade.

I Sverige finns också många andra myndigheter som har uppgifter som är av central betydelse för cybersäkerheten. Sveriges post- och telekommunikationsmyndighet PTS svarar för området för post och elektronisk kommunikation och bland annat för övervakningen av molntjänster. Polisen, Åklagarämbetet och Sveriges säkerhetstjänst ansvarar för utredningen av brott mot nät och cybersäkerhet som omfattas av strafflagarna. I fall som gäller skydd av personuppgifter är Sveriges dataskyddsmyndighet IMY (Integritetsskyddsmyndigheten) behörig myndighet.

Sveriges lagstiftning har utvecklats när det gäller cybersäkerheten, och särskilt lagstiftningen om nationell säkerhet från 2018 (Säkerhetsskyddslagen) ställer krav på de aktörer som arbetar med kritisk infrastruktur och utvidgar Säpos befogenheter i fråga om övervakningen. Till skillnad från Finland har inte Sverige beredskaps- och undantagslagstiftning som ökar regeringens makt i förhållande till riksdagen. I stället föreskrivs om juridiska grunder för beredskap för krisförhållanden och verksamhet i undantagsförhållanden i grundlagen (särskilt i Regeringsformen; 1974) och i den normala lagstiftningen. Enligt närhetsprincipen i modellen för krisledningen i Sverige bör man i en krissituation i mån av möjlighet svara på en krissituation på den lägsta möjliga förvaltningsnivån.

#### 5.2.1.2 Lagstiftning

I Sverige finns inte en heltäckande cybersäkerhetslag. Den juridiska ramen för cybersäkerheten har delats upp på flera olika lagar. På brott, såsom informationsnätsbrott tillämpas i Sverige strafflagen (Brottsbalken). Om terrordåd och cyberangrepp föreskrivs i Sveriges lag om ansvar för terroristbrott (Lag om straff för terroristbrott). Om behandlingen av personuppgifter när det gäller de statliga myndigheter som svarar för förebyggande, utredning och lagföring av brott föreskrivs i Sveriges lag om behandling av personuppgifter i samband med brott (Brottsdatalagen). På dem som tillhandahåller elektroniska kommunikationstjänster tillämpas i Sverige lagen om elektronisk kommunikation (Lag om elektronisk kommunikation). På vissa livsviktiga tjänster inom kritisk infrastruktur tillämpas Sveriges lag om informationssäkerhet för tillhandahållare av samhällsviktiga och digitala tjänster (Lag om informationssäkerhet för samhällsviktiga och digitala tjänster). Dessutom föreskrivs om vissa funktioner som anses viktiga för Sveriges nationella säkerhet i Sveriges lag om säkerhetsskydd (Säkerhetsskyddslag).

#### 5.2.1.3 Handräckning

I Sverige grundar sig den handräckning som försvarsmakten ger till polisen på förordningen om försvarsmakten (Förordning 2007:1266 med instruktion för Försvarsmakten), och det föreskrivs separat om handräckning för civil verksamhet, helikoptertransporter och förebyggande av terrorism. Lagen om handräckning för bekämpning av terrorism (Lag 2006:343 om Försvarsmaktens stöd till polisen vid terrorismbekämpning) möjliggör lämnande av handräckning till polisen samt till Sveriges underrättelse- och säkerhetstjänst Säpo.

#### 5.2.1.4 Samhällets kritiska funktioner

I Sverige definieras som samhällsviktiga funktioner sådana verksamheter, tjänster eller infrastrukturer, som upprätthåller eller säkerställer funktioner som är nödvändiga med tanke på samhällets grundbehov, värden eller säkerhet. MSB har publicerat anvisningar för identifiering av viktiga funktioner (Identifiering av samhällsviktig verksamhet: metod). I Sverige finns inga särskilt namngivna myndigheter som ansvarar för samordningen av alla nationellt viktiga åtgärder för hela Sverige. Länsstyrelserna och de centrala myndigheterna ska specificera de socialt viktiga funktionerna inom sina egna verksam-hetsområden. På nationell nivå definierar säkerhetsmyndigheterna vad som är viktigt inom deras egna ansvarsområden.

### 5.2.2 Norge

#### 5.2.2.1 Myndigheter

Norges cybersäkerhetscenter (Nasjonalt cybersikkerhetssenter) som grundades 2018 har till uppgift att fungera som nationell och internationell kontaktpunkt och samarbetsorgan för analys, utredning och konsultation gällande incidenter i samband med cybersäkerheten. De uppgifter som koncentrerats till cybersäkerhetsaktören betjänar samhällets tekniska operativa behov i anslutning till informations- och cybersäkerheten. Centret har samarbetspartner såväl inom näringslivet och försvaret som inom den offentliga förvaltningen.

På nationell nivå finns flera aktörer inom cybersäkerheten. För cybersäkerheten ansvarar särskilt justitie- och beredskapsministeriet, försvarsministeriet, ministeriet för lokal förvaltning och modernisering, kommunikationsministeriet samt utrikesministeriet. I normala förhållanden koncentreras samordningsansvaret för de civila cybersäkerhetsarrangemangen på justitie- och beredskapsministeriet och de verk som är underställda det, i huvudsak polisen och NSM: (Nasjonal sikkerhetsmyndighet), samt sektorvis på olika behöriga myndigheter, såsom Norges telekommunikationsmyndighet (Nasjonal kommunikasjonsmyndighet). NSM är den nationella säkerhetsmyndigheten, som utom för cybersäkerheten ansvarar för bland annat åtgärder för skydd av kritisk infrastruktur. NSM har ett betydande ansvar för den civila cybersäkerheten eftersom underställda detta verk är det nationella cybersäkerhetscentret och Nor-CERT (den nationella CERT-verksamheten) som hör till det.

Från försvarsförvaltningens synvinkel är de centrala myndigheterna försvarsministeriet och den militära underrättelsetjänsten som är underställd det NIS (Etterretningstjenesten) samt Norges försvarsmakts cyberförsarsavdelning som inledde sin verksamhet 2012. Till NIS:s uppgifter som en del av Norges armé hör att ge förhandsvarning om militärt hot som riktas mot Norge. I detta avseende hör till uppgiftsfältet också insamling av underrättelseuppgifter och uppgörande av hotanalyser över påverkan som riktas mot cyberförsvaret. Verket för civil beredskap DSB (Direktoratet for samfunnssikkerhet og beredskap), som är underställt justitie- och beredskapsministeriet, har en betydande roll i utvecklingen av den nationella beredskapsverksamheten och det civila försvaret. Till DSB:s uppgiftsfält hör upprätthållandet av en tväradministrativ lägesbild över risker och sårbarheter som är av nationell betydelse och verket har också ansvar för den nationella riskbedömningen och uppgörandet av en strategi över samhällets kritiska funktioner.

För att förbättra samarbetet och informationsutbytet mellan ministerierna och de myndigheter som är underställda dem har grundats en cyberkoordinationscentral FCKS (Felles cyberkordineringssenter), som sammanför Centralkriminalpolisen, den nationella cybersäkerhetsmyndigheten samt aktörerna inom militär och civil underrättelseverksamhet. I koordinationscentralen ingår utom de ovannämnda också Norges centralkriminalpolis Kripos, i samband med

vilken nyligen grundades en ny cyberbrottcentral (NC3). Cyberkoordinationscentralen sammanför civila och militära aktörer i syfte att bilda en gemensam och delad lägesbild över hot samt koordinera verksamheten för att svara på hoten.

För de centrala riskanalyser på nationell nivå som publiceras årligen svarar utom verket för civil beredskap säkerhetspolisen PST (Politiets sikkerhetstjeneste), Norges militära underrättelsetjänst NIS samt myndigheten för nationell säkerhet (NSM). Medan PST (interna hot, våldsamma rörelser, nationella intressen etc.), NIS (yttre hot och NSM (cybersäkerhet, kritisk infrastruktur etc.) typiskt koncentrerar sig på sektorvisa kriser och risker på kort sikt har DSB till uppgift att sammanställa denna information och göra en analys av helhetsbilden på längre sikt.

Norges modell för krisledning är centralt ledd och under det senaste decenniet har särskilt justitie- och beredskapsministeriets roll som allmän expert på civil krishantering vuxit. Som högsta beslutsnivå i krissituationer fungerar Norges utrikes- och säkerhetspolitiska ministerutskott, som behandlar de centrala sakfrågorna gällande säkerhetspolitik och beredskap. I princip är det ministerium till vars område situationen normalt hör ansvarigt för krissituationer. Det ansvariga ministeriet kan sammankalla en kriskommitté, till vars huvuduppgift hör att stärka koordineringen av olika förvaltningsområdens åtgärder och den praktiska stödverksamheten. Kriskommittén stöder krisberedskapsenheten som hör till justitie- och beredskapsministeriet. Landets regering har i sista hand ansvar för beredskapen och hanteringen av krissituationer.

#### 5.2.2.2 Lagstiftning

Norge har inte en heltäckande cybersäkerhetslag. Den juridiska ramen för cybersäkerheten har delats upp på flera olika lagar. På behandlingen av personuppgifter tillämpas den allmänna dataskyddsförordningen (GDPR) och den personuppgiftslag som utfärdades 2018. Genom den nationella säkerhetslagen från 2018 (Lov om nasjonal sikkerhet) strävar man efter att förebygga, observera och avvärja verksamhet som hotar den nationella suveräniteten. Syftet med lagen om elektronisk kommunikation (Lov om elektronisk kommunikasjon) är att tillhandahålla trygga och moderna kommunikationstjänster. Genom energilagen från 1990 (Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.) eftersträvas man att trygga tillgången på energi i Norge. Utom de ovannämnda lagarna finnsbestämmelser om cybersäkerhet också i andra lagar.

#### 5.2.2.3 Handräckning

I Norge fogades bestämmelserna om försvarsmaktens handräckning till polisen till polislagen (Lov om politiet) år 2015. Innehållet i bestämmelserna härleddes från den praxis som tillämpades innan lagen trädde i kraft, som byggde på försvarsmaktens anvisningar om handräckning till polisen, Enligt lagen kan handräckning ges för att förhindra och avvärja särskilt skadliga och omfattande angrepp. Handräckning kan ges för att skydda människors liv och hälsa, egendom och allmän trygghet vid olyckor, naturkatastrofer och i andra jämförbara situationer. Handräckningen ges i form av försvarsmaktens materiel och specialutbildade personal.

För handräckning gäller också en bestämmelse om handräckning (instruks om Forsvarets bistand til politiet), enligt vilken handräckning kan ges endast om handräckningsuppdraget är5 förenligt med försvarsmaktens primära uppgifter och polisens egna resurser är otillräckliga eller inte är tillgängliga för utförandet av uppgiften. Bestämmelsen förutsätter att försvarsmakten under handräckningsuppdraget agerar separat från polisen och självständigt sköter biståndsuppdraget.

#### 5.2.2.4 Samhällets kritiska funktioner

På nationell nivå baserar sig Norges beredskap på lagstiftning samt riskanalyser och –bedömningar. Verket för civil beredskap som är underställt justitie- och beredskapsministeriet har en betydande roll i bedömningen av risker och sårbarheter i samhället. I offentliggörandet av samhällets kritiska funktioner identifieras utom kritiska funktioner också det ministerium som svarar för respektive funktion, det objekt eller den tjänst som ska skyddas och de centrala myndigheter och andra aktörer som arbetar med dessa.

De kritiska funktionerna har definierats så att samhället inte skulle klara sig utan dem i mer än sju dagar utan att befolkningens funktionsförmåga äventyras. Funktionerna delas in i tre klasser, som är förvaltning och suveränitet, befolkningens trygghet och befolkningens funktionsförmåga. Dessutom upprätthåller justitie- och beredskapsministeriet en offentlig lista över de myndigheter och den nyckelpersonal som arbetar med de objekt och tjänster som ska skyddas. I Norge har utom kritiska funktioner också definierats så kallade viktiga funktioner, Till dessa hör bland annat hantering av farliga ämnen, medietjänster och begravningsverksamhet.

### 5.2.3 Tyskland

#### 5.2.3.1 Myndigheter

Som tyska förbundsrepublikens högsta cybersäkerhetsmyndighet fungerar BSI (Bunde-samt für Sicherheit in der Informationstechnik), vars uppgift är att förbättra statens. affärslivets och samhällets cybersäkerhet genom förebyggande, observation och reaktion. BSI är framförallt Tyska förbundsregeringens centrala tillhandahållare av informationssäkerhetstjänster och dess uppgift är att förhindra hot mot förbundsrepublikens datateknik och bistå andra myndigheter i frågor som rör datateknikens säkerhet. BSI svarar för cybersäkerheten på riksnivå och ger rådgivning och uppgör anvisningar om den digitala verksamhetsmiljöns säkerhet för förvaltningen, företag och privatpersoner. BSI är direkt underställd inrikesministeriet.

Det nationella cyberförsvarscentret Cyber-AZ (Das Nationale Cyber-Abwehrzentrum) grundades 2011 som en del av verkställandet av förbundsrepublikens regerings cybersäkerhetsstrategi. Cyber-AZ är samarbets-, kommunikations- och koordinationsforum för olika säkerhetsmyndigheter och det producerar en uppdaterad och heltäckande lägesbild över cybersäkerheten. Cyber-A har som mål att förbättra och försnabba informationsutbytet mellan de behöriga myndigheterna och inrättningarna samt effektivera koordineringen av skydds- och försvarsåtgärder i exceptionella informationssäkerhetssituationer. Till forumet hör åtta centrala myndigheter samt andra samarbetsmyndigheter.

#### 5.2.3.2 Lagstiftning

På cybersäkerheten tillämpas många olika bestämmelser i Tyskland. De viktigaste bestämmelserna som gäller cybersäkerheten är GDPR, förbundsrepublikens dataskyddslag och lagen om förbundsrepublikens dataskyddsverk (Gesetz uber das Bundesamt fur Sicherheit in der Informationstechnik, BSI-lagen). Dessutom föreskrivs om olika områden inom cybersäkerheten bland annat i lagen om telekommunikation (Telekommunikationsgesetz), banklagen (Kreditwesengesetz) och lagen om energiindustrin (Energiewirtschaftsgesetz). I datasäkerhetslagen (IT-Sicherheitsgesetz 2.0) föreskrivs om cybersäkerheten gällande kritisk infrastruktur.

I BSI-lagen från 2009 definieras BSI:s verksamhet. I lagen föreskrivs också om informationsutbytet mellan myndigheterna och BSI. Ett undantag när det gäller förmedlingen av information

är dock sådan information som inte får lämnas ut på grund av sekretessbestämmelserna eller avtal som ingåtts med parterna. Man får inte heller ingripa i skyddet av personuppgifter.

IT-Sicherheitsgesetz 2.0 har varit i kraft sedan maj 2021. Den utvidgar i betydande grad förordningen från 2015 (KRITIS-förordningen), eftersom det anges flera skyldigheter för operatörerna och staten ges mera befogenheter. BSI kan vid betydande störningar i samförstånd med den behöriga tillsynsmyndigheten i förbundsrepubliken kräva att operatörer eller organisationer för vitala infrastrukturer lämnar ut den information som behövs för att hantera störningen till verket, också personuppgifter.

5.2.3.3 Samhällets kritiska funktioner

I Tyskland har 2015 godkänts IT-Sicherheitsgesetz 2.0, som utgör grunden för skyddet av kritiska infrastrukturer. Upprätthållare av kritiska infrastrukturer, som denna lag tillämpas på, ska påvisa för förbundsrepublikens dataskyddsverk (BSI) att de uppfyller de datatekniska säkerhetsstandarderna. Aktörerna ska också anmäla datatekniska störningar i dataskyddet till BSI.

Den kritiska infrastrukturen har definierats i Tyskland på följande sätt: den kritiska infrastruktur som avses i lagen om förbundsrepublikens dataskyddsverk omfattar de inrättningar, system och delar av dem som hör till energi-, datateknik-, telekommunikations-, trafik-, hälso-, vatten-, livsmedels-, finansierings-, avfalls- och försäkringssektorn och som är nödvändiga med tanke på samhällets verksamhet, eftersom det om de kras-char eller störs leder till betydande brister i verksamheten eller risker för den allmänna säkerheten i Tyskland.

5.2.4 Storbritannien

5.2.4.1 Myndigheter

Storbritanniens National Cyber Security Center (NCSC) har inlett sin verksamhet 2016 och fungerar som Storbritanniens tekniska myndighet för cybersäkerhet och cyberhot. I Storbritannien ingår cybersäkerhetsmyndigheten som en del av det centraliserade säkerhetsverket, som utom för cybersäkerheten också ansvarar för bland annat den datatekniska underrättelseverksamheten, bekämpning av terrorism och extremrörelser, bekämpning av allvarlig och organiserad brottslighet samt stöd för informationssäkerheten. Centrets uppgift är att stöda nationella kritiska aktörer, den offentliga sektorn, företag och enskilda medborgare. Centret producerar information om cybersäkerhet och reagerar på störningar i cybersäkerheten för att minska de skador de orsakas organisationer och samhället. Till den centraliserade aktörens uppgifter hör bland annat hantering av störningar i cybersäkerheten, dvs. den så kallade CERT- och CIRT verksamheten. Centret är underställt Storbritanniens underrättelse- och säkerhetstjänst GCHQ (Government Communications Headquarters).

GCHQ är en underrättelse-, cybersäkerhets- och säkerhetsmyndighet, till vars uppgifter hör bekämpning av terrorism, förbättrande av cybersäkerheten och bekämpning av allvarlig och organiserad brottslighet. Myndigheten samlar underrättelseinformation och bedriver ett omfattande samarbete med internationella myndigheter. Storbritanniens utrikesminister svarar för GCHQ:s verksamhet, men GCHQ är inte underställd utrikesministeriet.

I Storbritannien svarar National Crime Agency (NCA) för utredning av allvarlig och organiserad brottslighet. Till NCA:s uppgifter hör brottsunderrättelse och internationellt samarbete för bekämpning och utredning av brottslighet. Till NCA:s uppgifter hör således också utredning av allvarlig och gränsöverskridande cyberbrottslighet. I Storbritannien kan organisationer anmäla om cyberangrepp till National Fraud and Cyber Crime Reporting Centre, som fungerar som

rapporteringscentral för bedrägerier och brottslighet på nätet. Vid sidan av rapporteringscentralen finns också National Fraud Intelligence Bureau (NFIB), vars uppgift är att analysera anmälningar om brott på nätet och leverera dem bland annat till den lokala polisen för utredning.

I Storbritannien fungerar också National Cyber Force som grundar sig på samarbete mellan försvars och underrättelsemyndigheterna. Till dess ansvarsområden hör verksamhet i cybermiljö för att avvärja hot mot Storbritannien och främja statens intressen i hemlandet och utomlands.

#### 5.2.4.2 Lagstiftning

I Storbritannien finns inte en heltäckande cybersäkerhetslag. Kommunikationslagen (The Communications Act 2003) innehåller skyldigheter som gäller cybersäkerheten, som tilllämpas på tillhandahållare av elektroniska nät och producenter av allmänna elektroniska kommunikationstjänster. I lagen om utredningsbefogenheter (Regulation of Investigatory Powers Act 2000) föreskrivs om vissa lagövervakningsbefogenheter, såsom övervakning av nätet. I IPA-avtalet (IPA 2016) utvidgas myndigheternas utredningsbefogenheter när det gäller cyberbrottslighet. I lagen om missbruk av datorer (Computer Missuse Act 1990) föreskrivs om olika brott som ansluter sig till datanät. Dessutom finns det många andra bestämmelser som behandlar cybersäkerhet.

I Storbritannien är enligt den allmänna dataskyddsförordningen personuppgifter sådana uppgifter med vilkas hjälp en fysisk person kan identifieras. Sådana uppgifter kan vara t.ex. IP-adresser, MAC-adresser och cookies på nätet. Om personuppgifter kan anonymiseras tillämpas inte längre den allmänna dataskyddsförordningen på dem i Storbritannien.

#### 5.2.4.3 Samhällets kritiska funktioner

I Storbritanniens cybersäkerhetscentrals ansvar ingår skydd av kritisk infrastruktur mot cyberangrepp. Centralen bedriver ett omfattande samarbete med Centre for the Protection of National infrastructuren (CPNI). CPNI har till uppgift att bistå och erbjuda hjälp till organisationer som ansvarar för skyddet av den nationella kritiska infrastrukturen.

Enligt Storbritanniens regerings officiella definition hör till den kritiska infrastrukturen sådan egendom och sådana anläggningar, system, nät och processer samt de anställda som använder dem, vilkas försvinnande eller utsättande för fara kan medföra betydande olägenhet för tillgången på tjänster, medföra avbrott i tjänsterna eller försvåra tillhandahållande av tjänster. I det ingår också tjänster som om de utsätts för avbrott kan leda till betydande förluster av människoliv eller betydande ekonomiska eller sociala konsekvenser eller betydande skada för den nationella säkerheten, försvaret eller statens verksamhet.

### 5.2.5 Frankrike

#### 5.2.5.1 Myndigheter

Frankrikes nationella cybersäkerhetsverk (ANSSI) är en myndighet för cybersäkerhet samt nät- och informationssäkerhet, vars uppgift är att främja fransk teknik, system och kompetens samt övervaka producenterna av de centrala tjänster som beskrivs nedan. Till den centraliserade myndighetens uppgifter hör bl.a. hantering av störningar i cybersäkerheten, dvs. den så kallade CERT- och CIRT verksamheten. ANSSI:s verksamhet effektiverades genom en militärprogrammeringslag som utfärdades i december 2013, där det föreskrivs om åtgärder genom vilka de livsviktiga operatörernas säkerhet förbättras och ANSSI beviljades av presidenten nya rät-

tigheter, genom vilka myndigheten i praktiken kan verkställa säkerhets- och övervakningsåtgärder gällande de livsviktiga operatörernas mest kritiska nät- och datasystem. Dessutom föreskrivs i lagen att mycket viktiga aktörer ska anmäla om farosituationer i systemen till ANSSI.

Dataskyddsmyndigheten CNIL (Commission Nationale de l'Informatique et des Libertés) övervakar Frankrikes dataskyddslag (FDPA) för behörig tillämpning av den allmänna dataskyddsförordningen för registeransvariga och handläggare av personuppgifter. CNI har betydande övervaknings- och utredningsbefogenheter i Frankrike. För tryggande av effektiv övervakning av. FDPA: kan CNIL utföra omfattande granskningar av alla registeransvariga och handläggare av personuppgifter.

Övervakningen av cybersäkerheten hör i Frankrike huvudsakligen till försvarsministeriets och inrikesministeriets förvaltningsområde. I Frankrike finns många polisenheter som är specialiserade på cybersäkerhet och som kan utföra brottsutredningar, informationsinsamling, spaningar, insamling av data och andra åtgärder som ingår i polisens befogenheter för att bekämpa cyberbrottslighet och utreda brott.

5.2.5.2 Samhällets kritiska funktioner

I Frankrike har i enlighet med nät- och dataskyddslagarna utsetts de centrala tjänsteproducenterna på olika områden, såsom energi-, trafik-, bank- och finansmarknadsstrukturerna, hälsovårdstjänsterna och apoteksbranschen, Sammanlagt 122 sådana aktörer har specificerats 2018, och antalet väntas öka i framtiden. Aktörerna tillhandahåller centrala tjänster som om de avbryts i betydande grad påverkar ekonomin eller samhällets verk-samhet. ANSSI stöder dessa aktörer för att säkerställa att de skyddas i enlighet med den planerade cybersäkerhetsutvecklingen. Den cybersäkerhetsram som tillämpas på de kritiska operatörerna togs i bruk 2013 genom lagen om dataskydd för livsviktiga infrastrukturer.

## 6 Remissvar

Propositionen sändes på remiss till 25 myndigheter och organisationer. Bland remissorganen fanns många ministerier, och de ombads sammanställa en samordnad syn inom sitt respektive förvaltningsområde. Också remissförfarandet bland intressebevakningsorganisationer inom näringslivet samt intressebevakningsorganisationer inom kritiska branscher var omfattande. Även Åland ombads yttra sig. Sammanlagt lämnades tolv yttranden.

Yttrande lämnades av finansministeriet, social- och hälsovårdsministeriet, inrikesministeriet, försvarsministeriet, justitieministeriet, Transport- och kommunikationsverket Traficom, Teknologiindustrin rf, Finnish Information Security Cluster FISC – Kyberala ry, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Finlands näringsliv rf, Finanssiala ry och Tieto- ja viestintätekniikan ammattilaiset TIVIA ry. En sammanfattning av yttrandena finns i statsrådets tjänst för projektinformations under nummer LVM071:00/2021. Här sammanfattas de viktigaste synpunkterna i yttrandena.

Remissorganen förhöll sig i huvudsak positiva till målen och förslagen, och propositionen ansågs viktig och behövlig. Det lämnades ändå en del ändringsförslag till förslaget, och vissa behov av preciseringar lyftes fram både i fråga om de föreslagna bestämmelserna och i fråga om motiveringen.

Försvarsministeriet lyfte i sitt yttrande fram allmänna synpunkter på att förslaget är en mellanfas med avseende på ett bredare cyberförsvar och att avsikten är att mer omfattande frågor ska lösas

inom det utredningsprojekt för cybersäkerhet som leds av inrikesministeriet och försvarsministeriet. Under den fortsatta beredningen kompletterades motiveringen med ett tillägg om behovet av ett mer omfattande beslutsunderlag i frågan och hur det aktuella förslaget förhåller sig till det.

När det gäller handräckning lyfte Transport- och kommunikationsverket fram att det krävs en närmare redogörelse för hur begreppet undanröjande av verkningar förhåller sig till myndigheternas behörighet, till exempel eftersom en begäran i ett läge där handräckning begärs ska hänföra sig till uppgiftsområdet för den myndighet som begär handräckning. Dessutom bör det klargöras hur förslaget förhåller sig till verksamheten inom den privata sektorn. Även Finlands näringsliv, Teknologiindustrin och FISC fäste uppmärksamhet vid detta i sina yttranden. Transport- och kommunikationsverket påpekade också att det föreslagna tillägget i slutet av lagförslaget, ”om inte något annat föreskrivs någon annanstans i lag”, är onödigt. Propositionen redogör nu närmare för vad undanröjande av verkningar innebär och hur detta förhåller sig till å ena sidan till myndigheternas befogenheter och å andra sidan till den privata sektorn. Dessutom har ”om inte något annat föreskrivs någon annanstans i lag” strukits. Försvarsministeriet föreslog dessutom vissa preciseringar i propositionsmotiven av vad handräckning innebär. Förslagen har beaktats i den fortsatta beredningen.

Justitieministeriet lyfte i fråga om bestämmelsen om handräckning fram behovet av att i stället för att bedöma dess förhållande till handräckning där maktmedel används granska den utifrån de allmänna förutsättningarna för handräckning. Dessutom bör Försvarsmaktens behörighet att sköta uppgiften enligt förslaget preciseras i motiveringen i enlighet med specialmotiveringen. Motiveringen har kompletterats i detta avseende under den fortsatta beredningen.

Finlands näringsliv, Teknologiindustrin och FISC föreslår att lagen får behövliga bestämmelser om assistans från enskilda som kan jämställas med handräckning. Eftersom observation, bekämpning och utredning av betydande och till sina verkningar allvarliga kränkningar av informationssäkerheten i praktiken kan kräva att de anställda vid alla relevanta myndigheter används för sina egna huvuduppgifter, kan man bli tvungen att skaffa den expertis som behövs på annat håll, framför allt hos aktörer inom näringslivet. Som exempel kan tjäna polislagens bestämmelser om bistånd, vars syfte är att i exceptionella lägen snabbt möjliggöra anlitande av för ändamålet lämplig utomstående hjälp. I detta fall är det fråga om Transport- och kommunikationsverkets rätt att få assistans av den privata sektorn mot ersättning enligt avtal. Förslaget är relativt omfattande och kräver utredningar och har därför inte kunnat beaktas i den fortsatta beredningen. Men remissvaren har delgetts inrikesministeriet och försvarsministeriet för deras mer omfattande utredningsarbete där samarbetet kring kränkningar av informationssäkerheten dryftas mer ingående.

Kärnan i remissvaren om informationsutbyte gällde tröskeln för tillämpning av ömsesidigt utbytet av information om betydande kränkningar av informationssäkerheten och den tillhörande begreppsapparaten. Särskilt begreppet kritiska branscher ansågs oklart och kräva precisering. Detta fördes fram både av myndigheter och av aktörer inom den privata sektorn. Justitieministeriet ansåg allmänt att den vaga formuleringen i förslaget förefaller skapa en spänning med avseende på det kvalificerade lagförbehållet i 10 § 4 mom. i grundlagen, och det framgår inte tydligt av motiveringen om avgränsningen alltid eller åtminstone till vissa delar ska grunda sig på utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden. När det gäller begreppet kritisk infrastruktur hänvisar justitieministeriet dessutom till vad grundlagsutskottet sagt i samband med förslaget till ändring av beredskapslagen. Finansministeriet ansåg att kritiska funktioner bör inbegripa statens skuld- och kassahantering. Också en mer entydig definition av kritisk infrastruktur efterlystes. Inrikesministeriet välkomnar en relativt hög tröskel för tillämpning av undantagsbestämmelser anses vara relativt hög av skäl som samman-

hänger med de grundläggande fri- och rättigheterna. Finlands näringsliv, Teknologiindustrin och FISC anser att definitionen i den föreslagna 319 a § är en utmaning. Bestämmelsen har ett välkommet syfte, men med beaktande av skyddet för de grundläggande fri- och rättigheterna bör bestämmelsen förutsättas vara så tydlig som möjligt. Exempelvis har begreppet samhällets kritiska funktioner inte ett fullständigt etablerat och noggrant avgränsat innehåll. Det föreslås att definitionen ska övervägas mer ingående.

Transport- och kommunikationsverket anser att förslaget bör finna en balans mellan å ena sidan möjliggörande av myndigheternas informationsutbyte och å andra sidan begränsningar av kommunikationens konfidentialitet eller sekretessgrunder. Verket anser att tröskeln för att tillämpa det som föreslås kan bli hög och i praktiken begränsa hur bestämmelsen kan utnyttjas. Transport- och kommunikationsverket fäster uppmärksamhet vid begreppet kritisk infrastruktur, som kan ge rum för tolkning eller begränsa tillämpningen i enskilda fall på ett oändamålsenligt sätt. Myndigheten föreslår att det i stället för kritisk infrastruktur kan vara motiverat att i större utsträckning tala om samhällets vitala funktioner, såsom 244 a § i lagen om tjänster inom elektronisk kommunikation redan gör. Verket hänvisar också till förarbetena till den nyligen genomförda ändringen av beredskapslagen. Dessutom tar det upp förslagen i personuppgiftslagarna för polisväsendet och Försvarsmakten. Enligt verket skulle förhållandet mellan 319 a § och lagarna om behandling av personuppgifter i fortsättningen göra det möjligt att trots sekretessbestämmelserna lämna ut personuppgifter till Transport- och kommunikationsverket beroende på lag antingen enligt behövlighetskriteriet eller nödvändighetskriteriet i delvis överlappande situationer med avseende på 319 a § i lagen om tjänster inom elektronisk kommunikation. Under den fortsatta beredningen har förslaget omformulerats så att det blivit mer exakt och då användes begreppet samhällets vitala funktioner i definitionen av undantagsförhållanden i ändringen av beredskapslagen. Förslagen i personuppgiftslagarna ändrar i praktiken inte det gällande rättsläget avsevärt. I sig är tillämpningssituationerna delvis överlappande, men med stöd av den föreslagna 319 a § går det att utbyta också annan information än sådan som anses vara personuppgifter.

Inrikesministeriet ansåg dessutom att motiveringen lämpligen bör kompletteras på så sätt att myndigheterna använder inkommen information inom ramen för sina egna behörighetsregler och att speciallagstiftningen är förenad med begränsningar som gäller utlämnande av vissa uppgifter (t.ex. biometriska kännetecken). Det behövs också bestämmelser om vidarelämnande av uppgifter. Motiveringen har kompletterats i enlighet med detta. Det har dock inte föreslagits några särskilda begränsningar för vidarelämnande av uppgifter, eftersom olika myndigheters verksamhet också bygger på nyttjande av internationella nätverk. Med beaktande av att kränkningar av informationssäkerheten är av gränsöverskridande karaktär kom man under den fortsatta beredningen fram till att det är motiverat att bevara möjligheten att utbyta information med dem där lagstiftningen redan i dagsläget möjliggör utbyte när informationssäkerheten kränks. Vidarelämnande av uppgifter är också strikt reglerat utifrån syfte och behov samt på så sätt att skyddet för förtroliga meddelanden och integritetsskyddet begränsas så lite som möjligt, vilket för sin del begränsar vidarelämnandet av uppgifter. I den fortsatta beredningen beaktades dock vissa begränsningar som gäller vidarelämnande av uppgifter och som framgår av motiveringen till det föreslagna 319 a § 3 mom.

Inrikesministeriet fäste uppmärksamhet vid att propositionen inte tar upp rätten till insyn enligt dataskyddslagstiftningen i fråga om uppgifter som fåtts med stöd av den lagstiftning som propositionen gäller. Exempelvis i fråga om polisen har den s.k. direkta rätten till insyn i egna uppgifter inskränkts i 42 § i lagen om behandling av personuppgifter i polisens verksamhet för att rätten till insyn inte ska äventyra utförandet av polisens lagstadgade uppgifter. Utförandet av de lagstadgade uppgifterna får inte heller äventyras av att en person via en annan myndighet får

tillgång till uppgifter som polisen lämnat ut och som omfattas av inskränkningen i rätten till insyn. Detta påpekande har lagts till i förslaget.

Försvarsministeriet har lyft fram frågan om hur entydigt det är IP-adresser ska tolkas som personuppgifter och påpekat att man bör undvika en alltför enkelspårig tolkning att så alltid är fallet. Ordalydelsen i motiveringen har därför preciserats något. Dessutom framförde ministeriet anmärkningar om att lagstiftningen inom dess förvaltningsområde kompletteras genom lagen om militär disciplin och brottsbekämpning inom försvarsmakten. Också detta beaktas nu i propositionen.

Social- och hälsovårdsministeriet påpekar att förslaget inte behandlar särskilt känsliga uppgifter och föreslår att förslaget kompletteras med en bestämmelse om radering av onödiga uppgifter. En bestämmelse om radering av onödiga uppgifter har fogats till förslaget och även motiveringen har kompletterats i enighet med detta.

Finanssiala, Finlands näringsliv, Teknologiindustrin och FISC understöder ett förbättrat informationsutbyte mellan myndigheterna, men anser att också den privata sektorn bör beaktas i informationsutbytet. Organisationerna anser att vara märkligt om myndigheterna utbyter information eller vidtar åtgärder utan att det berörda företaget får information eller får delta i utredningen. Dessutom understryker Finanssiala och Finlands näringsliv att förfarandena för informationsutbyte bör utformas så att de uppfyller kraven på informationssäkerhet, dataskydd och dokumentation. Genom kontinuerlig observation säkerställs dessutom att begärandena om information och svaren på dem är formellt och innehållsmässigt korrekta. När det gäller utländska myndigheter måste det säkerställas att informationsutbytet under alla omständigheter sker i enlighet med tillämpliga rättsliga krav, allmänna principer för dataskydd och god databehandlingspraxis. Analysen under den fortsatta beredningen gav vid handen att lagstiftningen om informationsutbyte i fråga om privata aktörer som blivit utsatta för kränkningar av informationssäkerheten inte innehåller motsvarande hinder som har upptäckts mellan myndigheterna. Det går att lämna ut omfattande uppgifter till privata aktörer med stöd av lagen om tjänster inom elektronisk kommunikation när kränkningen av informationssäkerheten gäller dem själva. Myndigheternas rätt att utbyta information vid kränkningar av informationssäkerheten utvidgas i praktiken till motsvarande nivå genom förslaget. Informationsutbytet utomlands sker alltid med specificerade aktörer enligt etablerade förfaranden och endast i behövlig omfattning. Detta är redan praxis.

Dessutom föreslår de ovan nämnda intressebevakningsorganisationerna att bestämmelsen preciseras så att information som lämnats ut inte får lämnas vidare till andra än de finländska myndigheter som nämns i paragrafen. När myndigheterna lämnar ut information till varandra ska de dessutom underrätta det berörda företaget vilka uppgifter som har lämnats ut samt när och till vem. Dessutom har det föreslagits en bestämmelse om utplåning av information som motsvarar 316 § 4 mom. Förslaget har kompletterats med en sådan bestämmelse. Under den fortsatta beredningen ansågs det inte ändamålsenligt att förbjuda vidarelämnande av information, i synnerhet eftersom det med tanke på utredningen av kränkningar av informationssäkerheten kan vara synnerligen väsentligt att behövlig information kan delas med exempelvis utländska partner. Attackerna kommer sällan från aktörer innanför landets gränser, och därför spelar det internationella samarbetet en betydande roll när det gäller att reda ut kränkningar av informationssäkerheten och också att förebygga framtida attacker.

När det gäller information som lämnas ut till utlandet föreslog Transport- och kommunikationsverket att också 319 § 2 mom. 2 punkten ändras i detta sammanhang så att det ska vara möjligt att lämna ut information exempelvis till Europeiska unionen och Nato för att förebygga eller

utreda kränkningar av informationssäkerheten som är riktade mot kommunikationsnät och kommunikationstjänster. FiCom lyfter fram att den gällande lagen (319 § 2 och 3 mom.) möjliggör bland annat utlämning av information som en datamängd och att där saknas kriterier för betydelse, konsekvens och nödvändighet, förbudet mot vidarelämnande och ett ovillkorligt användningsändamål. FiCom inser att förfarandet kan behöva förenklas, men villkoren för utlämnande bör skärpas. Dessutom lyfter FiCom fram att företagen till följd av skyddet för förtroliga meddelanden behöver få information när information lämnas ut, vilket innebär att Transport- och kommunikationsverket bör samarbeta med de företag vars information lämnas ut. En sådan bestämmelse finns i 5 mom., som enligt förslaget ska utgå, men verket bör åtminstone underrätta det företag vars information det är som har lämnats ut om vilka uppgifter som har lämnats ut samt när och till vem. Förslaget har kompletterats med ett omnämnande av EU och Nato. I fråga om FiComs syn på utlämning av information som en datamängd kan det påpekas att 319 § 3 mom. i den gällande lagen begränsar utlämnandet av uppgifter till utlandet med krav på behövlighets och på att skyddet av konfidentiella meddelanden och integritetsskyddet ska beaktas. Det är således inte under några omständigheter fråga om ospecificerad utlämning av information som en datamängd. Det är värt att notera att man i den nationella lagstiftningen inte kan definiera hur en myndighet i en annan stat använder information utan ett fördrag. I dagsläget begärs tillstånd för utlämnande av uppgifter i praktiken på förhand, och avsikten är inte att ändra denna princip ens i normala situationer.

När det gäller frivilligt utlämnande av information från kommunikationsförmedlaren sida till Transport- och kommunikationsverket påpekar social- och hälsovårdsministeriet att förslaget i princip är välkommet, men att det av propositionen inte framgår i vilka situationer och med vilka metoder kommunikationsförmedlaren på eget initiativ kan konstatera en sådan genomförd eller förutsebar kränkning av informationssäkerheten eller ett hot om en sådan kränkning i anslutning till vilken den kan lämna ut både förmedlingsuppgifter och meddelanden. Ministeriet påpekar att det bör föreskrivas om utplåning av särskilt känsliga uppgifter och uppgifter som är sekretessbelagda med stöd av annan lag och om förbud mot att använda uppgifterna för andra ändamål. När det gäller den fortsatta beredningen anser Transport- och kommunikationsverket att det är lämpligt att bedöma om förslaget behöver kompletteras med en bestämmelse som understryker att bara information som absolut behövs lämnas ut. Dessutom bör det övervägas om utlämnandet av information för tydlighetens skull ska begränsas till situationer där de uppgifter som lämnas ut hänför sig till en viss (misstänkt) störning som skadar informationssäkerheten. Förslaget bör till denna del också behandlas i motiveringen till lagstiftningsordningen med avseende på 10 § i grundlagen och granskas i förhållande till artikel 15 i direktivet om integritet och elektronisk kommunikation. Också Finanssiala och Finlands näringsliv föreslår att bestämmelsen avgränsas i enlighet med motiveringen. Ansträngningar har gjorts för att i förslaget öppna upp motiveringen för metoderna för utlämnande av information och behandlingen av känsliga uppgifter. Bestämmelserna har preciserats med de begränsningar som framgår av propositionsmotiven i enlighet med remissvaren.

TIVIA har som allmän kommentar till propositionen uttryckt sin oro över hur propositionen förhållande till dataskyddet och huruvida myndigheterna har tillräckliga åtkomstbegränsningar och åtkomsträttigheter, dvs. hur man säkerställer att obehöriga personer inte får tillgång till information i onödigt stor omfattning. Också kvalitetsrevisionens tillräcklighet och omfattning har lyfts fram. Vidare pekar TIVIA på behovet av en tydligare terminologi. Strävan har varit att i förslaget beakta dataskyddsfrågorna i så stor utsträckning som möjligt och under den fortsatta beredningen gjordes ytterligare påpekanden om dataskyddet. Myndigheterna arbetar i enlighet med kraven på dataskydd också i de situationer som avses i förslaget, och inga ändringar föreslås i fråga om detta.

Justitieministeriet fäste i sitt yttrande särskild uppmärksamhet vid motiveringen till lagstiftningsordningen. Ministeriet lyfte då fram behovet av att för det första komplettera motiveringen till den föreslagna 316 a § och bedöma dess förhållande till 10 § i grundlagen. För det andra ansågs det nödvändigt att göra en noggrannare åtskillnad mellan avvägningar om sekretessbelagda uppgifter ska utlämnas och avvägningar som gäller skyddet för konfidentiell kommunikation. Dessutom ansåg ministeriet att förhållandet mellan den föreslagna 319 a § och de andra bestämmelserna ställvis är oklart och till denna del behöver förtydligas. Det anser att det är fråga om en ny bestämmelse om utlämnande av information och att den delvis gäller sådana uppgifter som det inte är möjligt att lämna ut med stöd av den nuvarande regleringen. Att beskriva den föreslagna bestämmelsen som ett undantag från den gällande regleringen utgör ingen exakt beskrivning av förslaget till denna del. Under den fortsatta beredningen har man vinnlagt sig om att komplettera motiveringarna på det sätt som föreslås i yttrandet.

Justitieministeriet har dessutom påpekat att exempelvis känsliga uppgifter inte ligger utanför rätten att få information. Beredningen bör fortsätta med en analys av huruvida avsikten är att alla nämnda myndigheter ska kunna lämna ut eller få information för alla de ändamål som avses i paragrafen eller om det är möjligt att precisera bestämmelserna till denna del, menar ministeriet. Dessutom bör man avgöra om de informationsbehov som gäller hot om kränkningar är identiska med behovet vid en utförd kränkning av informationssäkerheten. Bestämmelsen har preciserats till vissa delar utifrån detta, även om det har ansetts befogat att i sak behålla samma omfattningen på den information som lämnas ut. Däremot har beskrivningen av de uppgifter som lämnas ut preciserats. Kränkningar av informationssäkerheten kan se ut på många sätt och de är oförutsägbara. Därför är det i praktiken mycket svårt att närmare specificera de uppgifter som behövs för utredningen och kan även leda till tillämpningsproblem, om den information som behöver fås utlämnad inte finns med i en detaljerad förteckning. Samma utmaning i fråga om kränkningarnas mångfald gäller också informationsutbytet vid hot om kränkningar. I sådana lägen är det svårt att på förhand bedöma vilken information som behöver bli föremål för utbytet.

Justitieministeriet har också fört fram att det behövs en mer ingående beskrivning av propositionens förhållande till den så kallade brandväggsregleringen, vars betydelse grundlagsutskottet underströk i samband med att underrättelselagstiftningen godkändes. Dessutom har det ansetts nödvändigt att i motiveringen till lagstiftningsordningen närmare ta upp skyddet för personuppgifter. Ministeriet har dessutom framfört enskilda behov av kompletteringar i motiveringen till olika bestämmelser. Dessa kompletteringsbehov har tillgodosetts i den fortsatta beredningen av propositionen.

Relativt få yttranden gällde propositionens egentliga konsekvenser, men Transport- och kommunikationsverket lyfte fram den eventuella negativa inverkan som en oklar terminologi kan ha på tillämpningen. Finlands näringsliv påpekade att konsekvenserna kan variera branschvis och att samarbetet inom en del branscher redan nu är relativt välfungerande och regelbundet. FiCom lyfte fram att det förblir oklart hur informationsutbyte mellan myndigheterna kommer att hjälpa ett företag i situationer där det har utsatts för en betydande kränkning av informationssäkerheten. Konsekvensbedömningen och motiven i övrigt har kompletterats i detta avseende.

Andra synpunkter som framfördes i yttrandena var den redan nämnda önskan att den privata sektorn bättre kopplas till situationer där informationssäkerheten kränks och förslaget att det görs en utredning av hindren för informationsutbyte mellan offentlig och privat sektor. Privata aktörer förde också fram principen om samservice i fråga om de olika anmälningsskyldigheterna, som det redan finns en hel del av. Förslag har också framförts om en helhetsbedömning av bestämmelserna om informationsutbyte i lagen om tjänster inom elektronisk kommunikation. De förslagen har inte förts vidare inom detta lagstiftningsprojekt, men de har presenterats för

inrikesministeriets och försvarsministeriets utredningsprojekt för cybersäkerhet, där olika ämnen behandlas mer omfattande och på mer allmän nivå.

## 7 Specialmotivering

### 7.1 Lagen om tjänster inom elektronisk kommunikation

**250 §** *Myndighetsabonnemang.* I 4 mom. föreslås en lagteknisk ändring som innebär att bestämmelsen flyttas till 316 § 5 mom. medan det gällande 250 § 4 mom. upphävs. Enligt det gällande 4 mom. tillämpas 316 § inte på sådan kommunikation som utövas i samband med skötsel av myndighetsuppgifter i myndighetsnät eller i kommunikationstjänsten med anknytning till myndighetskommunikation. Bestämmelsen flyttas till 316 § eftersom det är fråga om en begränsning av tillämpningen av den paragrafen och begränsningen nu blir lättare att hitta för den som ska tillämpa den än om den finns någon annanstans i samma lag. Ändringen är således lagteknisk och avsikten är inte att ändra det rådande rättsläget i fråga om begränsningen av paragrafens tillämpningsområde när det gäller myndighetsuppgifter.

**309 §** *Handräckning.* I 1 mom. föreslås en ändring som gäller handräckning som Försvarsmakten, polisen och skyddspolisen lämnar Transport- och kommunikationsverket. I övrigt ändras inte bestämmelserna om handräckning i momentet. Det är fråga om en specialbestämmelse i förhållande till bestämmelserna om handräckning av dessa myndigheter i polislagen (872/2011) och lagen om försvarsmakten (551/2007). På processen när det gäller att besluta om att lämna och begära handräckning tillämpas vad som i annan lag föreskrivs om sådant beslutsfattande. Momentet kompletteras med rätt för Transport- och kommunikationsverket att få handräckning av Försvarsmakten, polisen och skyddspolisen för att utreda betydande kränkningar eller allvarliga hot om betydande kränkningar av informationssäkerheten och deras verkningar. Enligt 11 § i lagen om försvarsmakten kan Försvarsmakten ge handräckning för skyddande av samhället enligt vad som föreskrivs i lagen om bekämpning av oljeskador (1673/2009) eller i någon annan lag. Polisen ska å sin sida enligt 9 kap. 1 § i polislagen på begäran ge andra myndigheter handräckning, om så föreskrivs särskilt. Handräckningen kan bestå av experthjälp, utrustning, lokaler eller anordningar.

De lägen där handräckning behövs och begärs gäller utredning av betydande kränkningar eller allvarligt hot om betydande kränkningar av informationssäkerheten och undanröjande av deras verkningar. Det kan bli aktuellt att begära handräckning i ett läge där Cybersäkerhetscentret vid Transport- och kommunikationsverket inte har tillräckliga tekniska resurser eller expertis för att utreda en kränkning av informationssäkerheten och undanröja dess verkningar och där Försvarsmakten, polisen eller skyddspolisen förfogar över resurser och förmågor som behövs för att svara mot denna brist och som hjälper Cybersäkerhetscentret att klara av sin uppgift. Begäran om handräckning ska gälla något som ligger inom ramen för den tillfrågade myndighetens uppgifter. Det kan vara fråga om en kränkning i vilken situation som helst där informationssäkerheten kränks på ett betydande sätt eller där den allvarligt hotas av en sådan kränkning, men handräckningen kommer att lämnas inom ramen för myndigheternas egna befogenheter. Det kan exempelvis övergå den ansvariga myndighetens faktiska förmåga att garantera rättigheterna för målorganisationens kunder, samarbetspartner eller andra berörda eller för andra som påverkas av attacken och således kräva till och med omfattande ytterligare samordnade åtgärder mellan myndigheterna.

Syftet med handräckningen är att stödja Cybersäkerhetscentrets kapacitet i exceptionella situationer, och därför utgörs handräckningen av experthjälp exempelvis genom personella resurser eller överlåtelse av anordningar, utrustning eller lokaler.

Med kränkning av informationssäkerheten avses all verksamhet som har skadliga konsekvenser för informationssäkerheten. Med informationssäkerhet avses enligt 3 § 28 punkten i lagen om tjänster inom elektronisk kommunikation administrativa och tekniska åtgärder genom vilka det säkerställs att information är tillgänglig endast för dem som har rätt att använda den, att informationen inte kan ändras av andra än dem som har rätt till detta samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen. Som en kränkning av informationssäkerheten betraktas en gärning eller händelse som leder till att äventyrar beståndsdelarna i informationssäkerheten för data, telekommunikation eller informationssystem eller någon av dem äventyras. En kränkning av informationssäkerheten kan leda exempelvis till att informationssystemet eller de anordningar eller tjänster som är beroende av det inte fungerar eller till obehörig åtkomst till uppgifterna i informationssystemet eller till att konfidentiella uppgifter i systemet äventyras på något annat sätt. De skadliga konsekvenserna av en kränkning kan gälla till exempel uppgifternas konfidentialitet, integritet och tillgänglighet eller funktionen hos en tjänst som tillhandahålls eller används med hjälp av informationssystemet. Som kränkning av informationssäkerheten ska åtminstone betraktas en sådan gärning som kan tillräknas gärningsmannen som brott och där rekvisiten är förenade med obehörigt intrång i informationssystemet eller med ändring, kopiering, radering eller annan obehörig behandling av uppgifterna i systemet. I strafflagen kriminaliseras kränkningar av kommunikationshemlighet, störande av post- och teletrafik, systemstörning och dataintrång.

Med betydande kränkning av informationssäkerheten avses en motsvarande it-säkerhetsincident som exempelvis tillämpas som tröskelvärde för rapporteringsskyldighet enligt NIS-direktivet. Handräckningen avses inte gälla situationer där kränkningen av informationssäkerheten endast orsakar ringa olägenhet och lindrig skada för informationssäkerheten. Vid betydande kränkningar eller allvarliga hot om betydande kränkningar av informationssäkerheten som kräver handräckning ska också deras eventuella verkningar beaktas. En betydande kränkning bör på förhand anses kunna orsaka samhället betydande skada eller olägenhet. Vid bedömningen av betydelsen ska man på det sätt som också avses i NIS-direktivet fästa uppmärksamhet vid verkningarnas utsträckning och varaktighet, geografiska omfattning samt kommunikationstjänsternas användbarhet, integritet eller kommunikationens konfidentialitet.

Handräckning ska också kunna lämnas när det är fråga om ett allvarligt hot om betydande kränkningar av informationssäkerheten. Med hot avses en situation som uppstår utan direkt avsiktligt mänskligt vållande och vars utnyttjande i skadligt syfte skulle medföra en kränkning av informationssäkerheten. Ett sådant allvarligt hot kan exempelvis vara en allvarlig sårbarhet i programvara eller system som används i stor utsträckning och där utnyttjande för brottsliga syften skulle medföra allvarliga skadliga verkningar för informationssäkerheten. Vid bedömningen av hur allvarligt hotet är ska man beakta sårbarhetens eller det övriga hotets beskaffenhet, dess exploaterbarhet i skadligt syfte och sannolikheten för skadliga verkningar samt hur allvarliga de skadliga verkningarna av exploateringen kan bli. För att det ska vara fråga om ett allvarligt hot om betydande kränkningar av informationssäkerheten ska verkningarna av att hotet realiseras vara lika allvarliga som en betydande kränkning av informationssäkerheten och sannolikheten för att hotet exploateras på ett skadligt sätt eller för att skadliga verkningar uppstår i övrigt vara stor. Således kan till exempel inte en betydande sårbarhet i sig komma i fråga, om risken för att den exploateras är liten eller närmast teoretisk och de skadliga verkningarna dessutom är osannolika eller det bara kräver små insatser för att förhindra dem. I praktiken kan det emellertid vara svårt att avgöra detta på förhand. Dessutom kräver förebyggande av skadliga verkningar att myndigheterna vidtar omfattande åtgärder eller har mycket avancerad teknisk kompetens, och därför kan handräckning i vissa mycket begränsade lägen vara motiverad också i förebyggande verksamhet vid hotfulla situationer, exempelvis för att förebygga skadliga verkningar av en allvarlig sårbarhet eller av ett allvarligt hot om en akut betydande kränkningar av informationssäkerheten. Det all-varliga hotet om en betydande kränkning av informationssäkerheten bör således

tolkas restriktivt och med betoning på sannolikheten för att sårbarheten exploateras, hur allvarlig den är och hur skadliga verkningarna i så fall blir.

Med utredning av kränkningar av informationssäkerheten eller hot om sådana kränkningar avses utredning av händelseförloppet och av de tekniska eller andra orsaker som ledde till kränkningen eller hotet om en kräkning. Med undanröjande av verkningarna av en kränkning av informationssäkerheten eller ett hot om en sådan avses de tekniska eller andra åtgärder som vidtas för att undanröja, lindra eller avvärja den fara eller andra konsekvenser för informationssäkerheten eller annan konfidentialitet i kommunikationen som den utredda kränkningen eller det utredda hotet medför. Med undanröjande av verkningar avses i synnerhet åtgärder för att säkerställa att kränkningen eller hotet inte skadar informationssäkerheten. När det gäller att undanröja verkningar måste det ändå beaktas att ansvaret för att verkningarna undanröjs i många situationer ligger hos den som utsatts för attacken eller dennes tjänsteleverantör. Myndigheterna kan stödja målorganisationerna i deras åtgärder för att undanröja verkningarna exempelvis genom att utreda vad som ligger bakom attackerna och tekniska fakta kring attackerna för att på så sätt stödja olika aktörer när verkningarna undanröjs. Med andra ord kan informationen i sådana situationer användas för att undanröja verkningar, även om myndigheten inte själv gör det.

Enligt det föreslagna *2 mom*. ska Transport- och kommunikationsverket i fortsättningen självt besluta om att lämna handräckning i stället för kommunikationsministeriet. Syftet är att bestämmelsen ska vara enhetlig med motsvarande bestämmelser i fråga om andra myndigheter, och samtidigt är det ändamålsenligt att myndigheten själv beslutar om utövandet av sin behörighet. Dessutom är det myndigheten själv som har den bästa uppfattningen om omfattningen och beskaffenheten på den handräckning den kan lämna, så det är lämpligt att den själv beslutar om handräckningen. Det är heller inte fråga om exempelvis handräckning som kräver maktmedel, och därför är det inte heller i detta avseende nödvändigt att kräva beslut på högre nivå. En annan ändring i momentet är att handräckningen till sin karaktär ska vara experthjälp, utrustning, lokaler eller anordningar på motsvarande sätt som i fråga om polisen, skyddspolisen och Försvarsmakten.

Bestämmelsen om kostnaderna för handräckningen flyttas enligt förslaget från nuvarande 2 mom. till ett nytt 3 mom. Omnämnandet av kostnaderna fungerar då som en reciprok bestämmelse i fråga om de kostnader som handräckning från olika myndigheter genererar och inte enbart som en bestämmelse som gäller handräckning som Transport- och kommunikationsverket lämnar. I övrigt föreslås inga ändringar i fråga om vem som ska står för dessa kostnader. Vidare föreslås i 3 mom. en bestämmelse om att en förutsättning för handräckning är att den inte äventyrar utförandet av andra viktiga uppgifter som ska skötas av den myndighet som lämnar handräckning. Det är fråga om en sedvanlig precisering av den nuvarande handräckningsregleringen, och den motsvarar de förutsättningar som under den senaste tiden tagits in i andra specialbestämmelser om lämnande av handräckning. Bestämmelsen motsvarar till exempel det villkor för handräckning som fogades till 89 § i lagen om smittsamma sjukdomar från och med den 22 februari 2021. I samband med att ändringen av 89 § i lagen om smittsamma sjukdomar behandlades förutsatte social- och hälsovårdsutskottet och förvaltningsutskottet att bestämmelserna om förutsättningarna för handräckning är tillräckligt exakta (ShUB 1/2021 rd och FvUU 29/2020 rd). Tillägget preciserar det gällande rättsläget till denna del.

Enligt förslaget blir *3 mom*. i den gällande lagen ett nytt 4 mom. Avsikten är att momentets innehåll huvudsakligen kvarstår oförändrat. Momentet avses emellertid i fortsättningen hänvisa till handräckning enligt både 1 och 2 mom., dvs. å ena sidan till situationer där Transport- och kommunikationsverket lämnar handräckning och å andra sidan till situationer där verket får handräckning av andra myndigheter. Enligt momentet ska lämnande av handräckning enligt 1 och 2 mom. inte berättiga Transport- och kommunikationsverket att till andra myndigheter

lämna ut information om meddelanden, förmedlingsuppgifter eller lokaliseringsuppgifter eller om konfidentiella radiosändningars innehåll och existens.

**316 §** *Behandling och utplåning av uppgifter om kommunikation och lokalisering*. Det föreslås att *avgränsningen av tillämpningsområdet i 5 mom*. kompletteras med den bestämmelse som upphävs i 250 § 4 mom. Det gällande 250 § 4 mom. gäller begränsning av tillämpningen av 316 § i fråga om kommunikation som utövas i samband med skötsel av myndighetsuppgifter i myndighetsnät eller i kommunikationstjänsten med anknytning till myndighetskommunikation. Ändringen är en förtydligande lagteknisk ändring där avgränsningen av tillämpningsområdet flyttas avgränsning i det gällande 316 § 5 mom. Avsikten är inte att ändra rättsläget till den del tillämpningen av 316 § på myndighetsverksamhet har avgränsats genom 250 § 4 mom., som upphävs.

**316 a §** *Kommunikationsförmedlares rätt att lämna ut information till Transport- och kommunikationsverket.* Den föreslagna paragrafen är ny. Enligt förslaget får en kommunikationsförmedlare frivilligt och på eget initiativ lämna ut information till Transport- och kommunikationsverket, om det behövs för att utreda eller förebygga kränkningar av eller hot mot informationssäkerheten. Kommunikationsförmedlare definieras i 3 § 36 punkten i lagen om tjänster inom elektronisk kommunikation. Med kommunikationsförmedlare avses således ett teleföretag, en sammanslutningsabonnent och en sådan annan aktör som förmedlar elektronisk kommunikation för andra än personliga eller med sådana jämförbara sedvanliga privata ändamål. Sådana är därmed också till exempel tillhandahållare av tjänster på virtuella privata nätverk (VPN) (HD 2022:23, punkt 13). Den information som lämnas ut är förmedlingsuppgifter eller uppgifter om meddelanden som kommunikationsförmedlaren har rätt att behandla med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation. Den paragrafen gäller kommunikationsförmedlarens åtgärder för att sörja för informationssäkerheten. Bestämmelsen medför ingen skyldighet att lämna ut uppgifter, utan den grundar sig på frivillighet. Bestämmelsen motsvarar vad som i 317 § 2 mom. i samma lag föreskrivs om radiostörningar.

Enligt 137 § 2 mom. i lagen om tjänster inom elektronisk kommunikation får elektroniska meddelanden och förmedlingsuppgifter lämnas ut endast till aktörer som har rätt att behandla uppgifterna i det aktuella fallet. Kommunikationsförmedlare får lämna ut förmedlingsuppgifter till varandra bland annat när genomförandet av informationssäkerhetsåtgärder förutsätter samarbete mellan teleföretag. Däremot innehåller lagen om tjänster inom elektronisk kommunikation i dagsläget ingen uttrycklig bestämmelse som ger kommunikationsförmedlare rätt att på eget initiativ till Transport- och kommunikationsverket lämna ut förmedlingsuppgifter om sådana kränkningar av informationssäkerheten som förmedlaren upptäcker eller innehållet i meddelanden, även om det hör till verkets lagstadgade uppgifter att samla in information om kränkningar av informationssäkerheten. En sådan situation kan uppstå till exempel när kommunikationsförmedlaren med hjälp av åtgärder enligt 272 § i lagen om tjänster inom elektronisk kommunikation har upptäckt en störning i informationssäkerheten eller ett meddelandeinnehåll som äventyrar informationssäkerheten. Bestämmelser om teleföretags anmälningsskyldighet vid betydande kränkningar av informationssäkerheten eller något annat som gör att en kommunikationstjänst inte fungerar eller väsentligen stör den finns i 275 § i lagen om tjänster inom elektronisk kommunikation. Även andra än teleföretag är emellertid kommunikationsförmedlare, varvid kommunikationens konfidentialitet och skyddet för personuppgifter inskränker möjligheten att lämna ut information för andra än teleföretag. Samtidigt har tröskeln för anmälan också i fråga om teleföretag satts vid betydande kränkningar av informationssäkerheten, vilket innebär att uppgifter om mindre kränkningar av informationssäkerheten ligger under denna tröskel. De uppgifterna kan vara viktiga exempelvis för förebyggande av kränkningar av informationssäkerheten.

Den gällande lagstiftningen innehåller i sig tanken att Transport- och kommunikationsverket kan begära förmedlingsuppgifter och meddelandeinnehåll av en kommunikationsförmedlare i fråga om en betydande kränkning av eller hot om en betydande kränkning av informationssäkerheten som verket fått kännedom om. Transport- och kommunikationsverket får emellertid inte nödvändigtvis kännedom om en sådan händelsen, eftersom redan informationen om att meddelandet existerar i princip omfattas av skyddet för förtroliga meddelanden. Kommunikationsförmedlaren kan också behöva hjälp av Cybersäkerhetscentret för att utreda en kränkning av informationssäkerheten som den upptäckt, såsom utredning av ett sabotageprograms funktionsprincip. Den nya bestämmelsen förtydligar utlämnandet av förmedlingsuppgifter och meddelandets innehåll till Cybersäkerhetscentret i en sådan situation. De oklarheter som råder i nuläget har i vissa fall fördröjt utredningen av vad som hänt, när kommunikationsförmedlaren inte lämnat information förrän efter det att på varandra följande begäranden om information har gjorts med stöd av 316 § 2 mom.

Med information som lämnas ut avses exempelvis information om meddelanden som innehåller eller sprider sabotageprogram och förmedlingsuppgifter om avsändare eller ledningsservrar. Information kan också lämnas ut om upptäckta överbelastningsattacker och om föremålen för dem. Transport- och kommunikationsverket kommer att kunna använda information som lämnas ut med stöd av förslaget för att skapa sin nationella lägesbild exempelvis när det gäller inkommen information om överbelastningsattacker. Dessutom kommer innehållet i meddelandena att kunna användas för att identifiera och spärra liknande meddelanden vars syfte är att sprida sabotageprogram. Utlämnande av information om meddelanden är också viktigt för att förebygga sms-kampanjer som döljer sabotageprogram. Den information om innehållet i ett meddelande som avses i paragrafen avser således i princip sådana uppgifter som med tanke på konfidentiell kommunikation är av mindre betydelse, såsom automatiskt skapade meddelandeinnehåll som främst innehåller eller sprider sabotageprogram eller kommandon som är skadliga på annat sätt. Bestämmelsen medger också automatiskt utlämnande av information i sådana fall där de kriterier för utlämnande av information som kommunikationsförmedlaren bestämt är uppfyllda i fråga om de åtgärder som förmedlaren vidtar med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation.

Bestämmelser om de allmänna behandlingsprinciperna för kommunikationsförmedlare finns i 137 § i lagen om tjänster inom elektronisk kommunikation. Till dessa hör behandling endast i den omfattning som syftet kräver och minsta möjliga begränsning av integritetsskyddet och skyddet för förtroliga meddelanden. Till behandlingsprinciperna hör dessutom att uppgifter får lämnas ut endast till dem som har rätt att behandla uppgifterna och att uppgifterna ska förstöras efter behandlingen, om inte något annat föreskrivs i lag. Enligt 137 § 4 mom. får meddelanden och förmedlingsuppgifter behandlas endast av personer som handlar för kommunikationsförmedlarens eller abonnentens räkning och som behandlar meddelanden och förmedlingsuppgifter för sådana ändamål som särskilt föreskrivs i 17 kap. i lagen om tjänster inom elektronisk kommunikation. Enligt förslaget ska 316 a § förtydligas genom en hänvisning till det som 137 § föreskriver om allmänna behandlingsprinciper för kommunikationsförmedlare. Dessutom föreslås det att sekretessen enligt 319 § i lagen om tjänster inom elektronisk kommunikation ska utsträckas också till uppgifter som erhållits med stöd av 316 a §. Avsikten är att också sådana uppgifter om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter eller konfidentiella radiosändningars innehåll och existens som eventuellt lämnats ut med stöd av 316 a § ska vara sekretessbelagda hos myndigheten i enlighet med huvudregeln i lagen om tjänster inom elektronisk kommunikation.

Information som erhållits med stöd av förslaget får lämnas vidare endast på det sätt som i 319 § föreskrivs om utlämnande av uppgifter om kommunikation och förmedling. Dessutom får

information lämnas ut till andra myndigheter i enlighet med den föreslagna 319 a §, dvs. i praktiken endast i särskilt exceptionella situationer.

**319 §** *Tystnadsplikt och utlämnande av information som gäller meddelanden*. Det föreslås att det till 1 mom. fogas ett omnämnande av den föreslagna 316 a §. Enligt momentet ska de uppgifter som Transport- och kommunikationsverket och dataombudsmannen har fått och skaffat om meddelanden, förmedlingsuppgifter, och lokaliseringsuppgifter samt om innehållet i och existensen av konfidentiella radiosändningar vara sekretessbelagda. Det föreslagna tillägget innebär att sekretessen enligt 319 § också gäller uppgifter om meddelanden eller förmedlingsuppgifter som erhålls med stöd av den föreslagna 316 a §. Med stöd av den gällande 319 § och förarbetena till den är huvudregeln att Transport- och kommunikationsverket och dataombudsmannen ska hemlighålla sådana uppgifter om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter och innehållet i och existensen av konfidentiella radiosändningar som de fått med stöd av lagen om tjänster inom elektronisk kommunikation (RP 221/2013 rd, s. 232). Eftersom kommunikationsförmedlarna med stöd av den föreslagna 316 a § får rätt att på eget initiativ lämna ut dessa uppgifter till Transport- och kommunikationsverket bör det föreskrivas att den huvudregel om sekretess som avses i 319 § också ska gälla uppgifter som erhållits med stöd av 316 a §, så att uppgifterna inte blir offentliga. I enlighet med det föreslagna tillägget till 1 mom. är sekretess huvudregeln också i fråga om de uppgifter som lämnas ut med stöd av 316 a § och som avses i bestämmelsen, och avvikelser från huvudregeln ska kunna göras endast i de situationer som uttryckligen anges i lag.

I *2 mom. 1 punkten* föreslås en lagteknisk ändring där hänvisningen till punkterna i 316 § 2 mom. stryks. I fortsättningen hänvisas det endast till hela momentet. Ändringen saknar betydelse i fråga om den praktiska tillämpningen. Enligt förslaget ska 2 punkten kompletteras med en möjlighet att lämna ut uppgifter också till aktörer som hanterar kränkningar av informationssäkerheten inom Europeiska unionen och Nordatlantiska fördragsorganisationen Nato. Det rör sig i praktiken om deras incidenthanteringsorganisationer (CERT-funktioner). Den gällande 2 punkten gör det möjligt att lämna ut uppgifter till myndigheter eller andra motsvarande aktörer som är verksamma i andra stater, men inte till internationella organisationer. Bestämmelsen behöver preciseras med det föreslagna tillägget, eftersom utlämnande av uppgifter kan behövas i vissa lägen när man beaktar Finlands deltagande i EU:s och Natos verksamhet, i synnerhet deras CERT-funktioner, där man utreder bland annat kränkningar av informationssäkerheten och hot om sådana kränkningar. På samma sätt som hittills ska uppgifter kunna lämnas ut endast till sådana institutioner, organ eller byråer vars uppgift är att förebygga eller utreda sådana kränkningar av informationssäkerheten som är riktade mot kommunikationsnät och kommunikationstjänster. Liksom tidigare begränsar 3 mom. den utsträckning i vilken information får lämnas ut. Enligt 3 mom. får information lämnas ut endast i den utsträckning som behövs för att förebygga och utreda kränkningar av informationssäkerheten, och vidare får utlämnandet inte begränsa skyddet av konfidentiella meddelanden och integritetsskyddet mer än vad som är nödvändigt. Inga ändringar föreslås i de gällande 3 och 4 mom.

Enligt förslaget upphävs *5 mom*. I fortsättningen kommer Transport- och kommunikationsverket självt att bestämma till vilka i 2 § 2 mom. avsedda aktörer det kan lämna ut förmedlingsuppgifter och andra uppgifter som det fått i samband med kränkningar av informationssäkerheten. Transport- och kommunikationsverket har själv de bästa instrumenten för att bedöma till vilka i andra stater verksamma myndigheter eller andra motsvarande aktörer som har till uppgift att utreda kränkningar av informationssäkerheten det kan lämna ut information som det innehar.

**319 a §** *Utlämnande av information vid betydande kränkningar av eller hot mot informationssäkerheten.* Den föreslagna paragrafen är ny. Avsikten är att genom en specialbestämmelsen

om informationsutbyte mellan myndigheter komplettera de andra bestämmelserna om informationsutbyte till de delar som de är förenade med begränsningar som gäller informationsutbyte. Den föreslagna bestämmelsen inskränker inte annan gällande lagstiftning om utbyte eller användning av information. Enligt förslaget ska Transport- och kommunikationsverket, polisen, skyddspolisen och Försvarsmakten trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter ha rätt att till varandra lämna ut nödvändiga uppgifter som gäller betydande kränkningar eller allvarliga hot om betydande kränkningar av informationssäkerheten. Uppgifter får lämnas ut i en situation där konsekvenserna av en betydande kränkning eller ett allvarligt hot om en betydande kränkning av informationssäkerheten gäller sådana vitala samhällsfunktioner som räknas upp i paragrafen eller informationsmaterial som gäller dessa funktioner. Avsikten är att täcka in de kränkningar av informationssäkerheten som är av allvarlig natur.

Med betydande kränkning av informationssäkerheten, hot mot informationssäkerheten, utredning och undanröjande av verkningar avses samma saker som i motiven till 309 §. Ett ytterligare villkor för tillämpningen är att konsekvenserna av kränkningen gäller de vitala samhällsfunktioner som räknas upp i paragrafen. Den föreslagna bestämmelsen täcker också in situationer där det finns en statlig aktör eller en stark misstanke om en statlig aktör. Vidare inbegrips också situationer där en statlig aktör anlitar eller med fog kan misstänkas anlita en ickestatlig aktör för att uppnå sina syften.

Enligt det föreslagna *1 mom*. får Transport- och kommunikationsverket, polisen, skyddspolisen och Försvarsmakten utbyta information med varandra. Utbytet kan ske ömsesidigt både på eget initiativ och på begäran av någon av myndigheterna i syfte att utföra lagstadgade uppgifter som gäller kränkningar av informationssäkerheten och möjliggöra en så smidig koordination av situationen som möjligt och samordning av verksamheten. Myndigheternas lagstadgade uppgifter i anslutning till kränkningar av informationssäkerheten beskrivs närmare i avsnittet om beskrivning av nuläget.

Förslaget medger utbyte vilken all nödvändig information för utredning av en eller flera kränkningar av eller hot mot informationssäkerheten. I praktiken kommer det att röra sig om uppgifter om kommunikation, förmedlingsuppgifter och attacker, men eventuellt också andra uppgifter. Det har inte ansetts möjligt att i detalj avgränsa innehållet i de uppgifter som lämnas ut till vissa uppgifter. Det beror på att de situationer där informationssäkerheten kränks kan variera stort i fråga om beskaffenhet och egenskaper, och alla dessa situationer kan inte förutses exakt.

Den information som en myndighet lämnar ut med stöd av paragrafen kan härröra från vilken information som myndigheten fått i sin verksamhet och som det är nödvändigt att inkludera i utbytet i den berörda situationen. I fråga om Transport- och kommunikationsverket kan det exempelvis röra sig om uppgifter som erhållits utifrån inkomna anmälningar eller uppgifter som erhållits via en övervakningstjänst. För polisens del kan det vara fråga om information som fåtts genom polisanmälningar eller teletvångsmedel. I fråga om skyddspolisen eller Försvarsmakten kan det exempelvis röra sig om information som inhämtats med stöd av egna befogenheter. Utlämnandet av uppgifter ska begränsas till uppgifter som är nödvändiga bara för den mottagande myndighetens verksamhet i syfte att utreda, förebygga eller undanröja verkningarna av betydande kränkningar av informationssäkerheten eller allvarliga hot om sådana. Myndigheterna ska använda informationen inom ramen för sina behörighetsbestämmelser. Det kan också röra sig om personuppgifter. Förslaget möjliggör i sig också utlämnande av känsliga uppgifter, men i praktiken behöver information som inbegriper sådana uppgifter inte utbytas mellan myndigheterna, eftersom exempelvis känsliga uppgifter som framgår av innehållet i ett meddelande saknar betydelse för utredningen av en kränkning av informationssäkerheten och därför lämnas dessa uppgifter inte ut.

Information får enligt förslaget lämnas ut mellan myndigheterna trots sekretessbestämmelserna. Detta gäller för det första uppgifter som är sekretessbelagda med stöd av offentlighetslagen. Polisens, skyddspolisens och Försvarsmaktens sekretessreglering bygger huvudsakligen på den. Dessutom innebär detta avvikelse från kommunikationens och förmedlingsuppgifternas konfidentialitet enligt 136 § i lagen om tjänster inom elektronisk kommunikation samt från skyldigheten till sekretess enligt lagens 319 § 1 mom. i fråga om uppgifter som skaffats med stöd av 316, 316 a och 317 § om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter om innehållet i och existensen av konfidentiella radiosändningar. Den föreslagna bestämmelsen medger också avvikelse i fråga om sådana uppgifter från utländska myndigheter som avses i 318 § 6 mom. i samma lag, dock med beaktande av begränsningarna i det föreslagna 319 a § 3 mom. För skyddspolisens och Försvarsmaktens del kan det vara fråga om begränsningar som gäller anmälan om brottsmisstanke. För dem finns särskilda bestämmelser om kriterier för brottens allvarlighet i de situationer där uppgifter måste lämnas ut för brottsbekämpning. Bestämmelser om detta finns i 79 § i lagen om militär underrättelseverksamhet och i 5 a kap. 44 § i polislagen. I praktiken är det ytterst sannolikt att gärningarna i de situationer som avses i förslaget är så pass allvarliga att kriterierna för brottens allvarlighet blir uppfyllda i alla fall. För polisens del kan det också vara fråga om utlämnande av information som inhämtats med hemliga tvångsmedel. Informationen kan ha inhämtats exempelvis genom systematisk observation, teleövervakning, teleavlyssning eller teknisk observation av utrustning, men när man beaktar de olika situationer där information kan behöva inhämtas kan det också vara fråga om andra metoder för informationsinhämtning 10 kap. i tvångsmedelslagen eller 5 kap. i polislagen. Bestämmelsen innebär också avvikelse från de begränsningar som uppställts för användning av överskottsinformation i 10 kap. 55 och 56 § i tvångsmedelslagen. I fråga om sådan information är det värt att notera att den med stöd av den gällande tvångsmedelslagen får användas också för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada. I praktiken är gärningarna i de situationer som avses i förslaget mycket sannolikt så pass allvarliga att kriterierna för brottens allvarlighet blir uppfyllda i alla fall, och det kan också vara fråga om att förhindra en sådan betydande fara eller skada som beskrivs ovan. I speciallagstiftning finns också exempelvis begränsningar som gäller utlämnande av information som gäller biometriska uppgifter, men de är emellertid inte direkt relevanta med avseende på utredning av kränkningar av informationssäkerheten.

Eftersom polisen ska bekämpa brott kommer den att använda information som erhållits med stöd av bestämmelsen för att utföra sina allmänna uppgifter, såsom att trygga rätts- och samhällsordningen, skydda den nationella säkerheten, upprätthålla allmän ordning och säkerhet och förebygga, avslöja och utreda brott. Polisen kommer att använda informationen exempelvis för att välja hur hemliga metoder för inhämtande av information ska inriktas. Erhållen information kommer att användas vid utredning av databrottslighet och också för att upprätthålla den nationella lägesbilden över itbrott. Skyddspolisens behov av information bygger särskilt på skyddet av den nationella säkerheten, såsom att upptäcka, förhindra och avslöja olaglig underrättelseinhämtning och påverkan som avser datanät. Skyddspolisen kan använda den information som fås med stöd av förslaget för att välja hur den civila underrättelseverksamheten ska inriktas och utreda vad som ligger bakom kränkningar av informationssäkerheten samt motiven till och konsekvenserna av sådana kränkningar för att kunna ta fram beslutsunderlag för statsledningen och andra myndigheter.

Försvarsmakten svarar för Finlands militära cyberförsvar som en del av den nationella cybersäkerheten och dess lagstadgade uppgifter. Uppgiften kräver en aktuell lägesbild. Dessutom måste Försvarsmakten kunna analysera sådana kränkningar av och hot mot informationssäkerheten som riktar sig mot kritiska funktioner för landets försvar eller mot försvarssystemet. Dessutom har Försvarsmakten tillgång till information, kompetens och utrustning som fokuserar särskilt

på dessa analyser av de allra mest krävande kränkningarna av och hoten mot informationssäkerheten. Genom analys samt identifiering och platsbestämning av den som kan ha utfört kränkningen blir informationen en del av Försvarsmaktens lägesbild, som används för att upptäcka och identifiera statliga och andra hotfulla aktörer. Utifrån lägesbilden kan nödvändiga åtgärder vidtas för att identifiera statliga och andra hotfulla aktörer och för att förhindra att de får tillgång till nyckelsystem och kärnuppgifter i försvarssystemet eller avvärja hotfulla aktörers insatser mot dessa. Försvarsmakten kommer att använda den information som erhållits med stöd av förslaget för att förebygga, avslöja och utreda brott och även exempelvis för att rikta in hemliga metoder för inhämtande av information till den del som de hör till Försvarsmaktens lagstadgade uppgifter på samma sätt som beskrivs i fråga om polisen. Försvarsmaktens behov av att bedriva militär underrättelseinhämtning hänför sig på samma sätt som skyddspolisens inhämtning av civila underrättelser till att utföra de uppgifter som anges i lagen om militär underrättelseverksamhet. Den information som fås med stöd av förslaget kan användas för att rikta in de metoder för underrättelseinhämtning som används inom den militära underrättelseverksamheten och för att utreda vad som ligger bakom kränkningar av informationssäkerheten samt motiven till och konsekvenserna av sådana kränkningar för att den militära underrättelseverksamheten ska kunna ta fram beslutsunderlag för statsledningen och för utförande av i lag särskild nämnda uppgifter för Försvarsmakten.

Transport- och kommunikationsverkets behov av information gäller teknisk utredning av kränkningar av eller hot mot informationssäkerheten och till förebyggande och upptäckt av sådana situationer. Det kommer för sin del att stödja också andra myndigheters verksamhet. Dessutom ska verket med hjälp av erhållen information skapa en nationell lägesbild av cybersäkerheten. Men Transport- och kommunikationsverket kan också bidra till att komplettera och berika information som andra myndigheter skaffat på annat sätt utifrån sin egen lägesbild, och då är det möjligt att få en mer detaljerad beskrivning av det övergripande läget.

Enligt förslaget ska uppgifter få lämnas ut när en betydande kränkning av informationssäkerheten har eller hotar ha allvarliga skadliga konsekvenser för det allmännas beslutsförmåga, myndigheternas verksamhetsförutsättningar, den nationella säkerheten, försvaret eller andra kritiska samhällsfunktioner. Det rör sig om funktioner där en kränkning av informationssäkerheten eller ett allvarligt hot om en sådan orsakar eller hotar att orsaka betydande skada för samhällets möjligheter att fungera.

*I 1 punkten* avses med det allmännas beslutsförmåga i huvudsak samma sak som i regeringens proposition med förslag till lagar om ändring av beredskapslagen och 79 § i värnpliktslagen (RP 63/2022 rd, s. 42). Med hot, händelser eller verksamhet som påverkar det allmännas beslutsförmåga avses således åtgärder som syftar till att förhindra eller på något annat sätt medföra avsevärd olägenhet för de högsta statsorganens, dvs. riksdagens, republikens presidents eller statsrådets, beslutsfattande eller verksamhet. Det kan också vara fråga om hot mot beslutsförmågan hos andra myndigheter som är viktiga för utredning av kränkningar av informationssäkerheten, dvs. polisen, skyddspolisen, Försvarsmakten och Transport- och kommunikationsverket. Det kan exempelvis vara fråga om störningar mot sådana informations- och kommunikationstekniska tjänster och informationssystem som är viktiga för beslutsprocesserna eller om datainträng, spridning av sabotageprogram eller spionprogram, överbelastningsattacker eller manipulation av omröstnings- eller valresultat.

Med risk för myndigheternas verksamhetsförutsättningar avses att myndigheternas möjligheter att sköta sina lagstadgade uppgifter äventyras. En sådan risk kan realiseras till exempel genom en kränkning av eller ett hot mot informationssäkerheten i den offentliga sektorns digitala tjänster.

Med nationell säkerhet avses *i 2 punkten* exempelvis verksamhet som hotar människors liv eller hälsa eller vitala samhällsfunktioner och som kan skada Finlands internationella relationer, ekonomiska intressen eller andra viktiga intressen. Även underrättelseverksamhet som avser utländska förhållanden avses. Också försvaret har traditionellt ansetts höra till kärnan av begreppet nationell säkerhet, men för tydlighetens skull nämns försvaret uttryckligen i den föreslagna paragrafen vid sidan av den nationella säkerheten. Med verksamhet som hotar den nationella säkerheten avses i princip verksamhet som inte i första hand riktar sig mot någon som individ utan mer allmänt mot samhället och dess mänskliga gemenskap (se RP 198/2017 rd).

Med allvarliga konsekvenser för försvaret avses i 2 punkten att funktioner som är av betydelse för Finlands försvar lider skada. Till dessa funktioner hör till exempel de ledningssystem som Försvarsmakten använder och de ingående informationssystemen samt myndighetsnät eller andra datakommunikationsförbindelser. På försvaret inverkar också leveranskedjor och service som är kopplade till försvarsutrustning.

Enligt *3 punkten* får information utbytas också när de skadliga konsekvenserna av en betydande kränkning av informationssäkerheten gäller nödvändiga tjänster inom social- och hälsovården eller räddningsväsendet. Konsekvenserna kan antingen direkt eller indirekt äventyra patientsäkerheten exempelvis via system eller nätuppkopplad hälso- och sjukvårdsutrustning eller nätuppkopplade vårdsystem. För räddningsväsendets del kan konsekvenserna vara till exempel sådana fördröjningar eller hinder när det gäller att utföra räddningsuppgifter som exempelvis beror på systemstörningar i förmedlingen av larm eller annan kommunikation inom räddningsväsendet eller störningar i tjänsterna för platsbestämning.

I *4 punkten* nämns energi-, vatten-, livsmedels- och läkemedelsförsörjningen och andra nödvändiga nyttigheter. Upprätthållandet av dessa funktioner bygger i stor utsträckning dels på faktisk produktion, dels på olika informationssystem för processförvaltning. Energisektorn är särskilt viktig när det gäller att upprätthålla samhällsfunktionerna. Störningar i energisektorn får omfattande följdverkningar också på andra vitala funktioner. Som kritiska funktioner inom sektorn kan betraktas olika energikällor och produktionsstrukturer, bränslen, el- och värmeproduktion samt överförings- och distributionssystem. Också vattentjänster, livsmedel och läkemedel kan lätt utsättas för skadliga konsekvenser, antingen genom attacker under tillverkningsprocessen eller genom attacker mot distributionen. Andra nödvändiga nyttigheter varor kan inbegripa exempelvis råvaruförsörjningen för att upprätthålla nödvändig industriproduktion.

Enligt *5 punkten* är nödvändiga betalnings- och värdepapperstjänster vitala samhällsfunktioner. Till dessa tjänster hör tillhandahållande av finans- och försäkringstjänster, all betalningsförmedling, clearing-, leverans- och förvaringsverksamheten inom värdepapperssektorn, kontantförsörjningen, infrastrukturen för kortbetalningar och de finansiella funktionerna inom dagligvaruhandeln. Betalnings- och värdepapperstjänsterna fungerar numera i hög grad i webbmiljö med hjälp av olika it-system och är därför också känsliga för attacker. Exempelvis har störningar i betalningsförmedlingarna omfattande konsekvenser för samhällets funktionsförmåga från individnivå till organisationsnivå och sträcker sig ända till statens betalningssystem.

Enligt *6 punkten* får myndigheterna utbyta information också om en kränkning av informationssäkerheten har allvarliga konsekvenser för tillgången till samhällets kritiska trafik- och kommunikationstjänster. Trafiktjänsterna och deras styrsystem är till exempel livsviktiga för livsmedelslogistiken såväl på land och till sjöss som i luften. Dessutom har exempelvis systemet för automatisering av trafiken betydande konsekvenser för trafiksäkerheten. I praktiken måste de tillhörande kommunikationstjänsterna och kommunikationsnäten finnas på plats för att systemen för alla dessa funktioner ska kunna fungera. Kränkningar av informationssäkerheten för de

allmänna kommunikationstjänsterna kan på samma sätt som i fråga om energisektorn ha långtgående spridningseffekter på flera olika branscher.

Den föreslagna *7 punkten* nämner särskilt informations- och kommunikationstekniska tjänster och tillhörande informationsmaterial som upprätthåller de funktioner som räknas upp i 1–6 punkten. Det är i sig klart att en betydande kränkning av informationssäkerheten i allmänhet uttryckligen är riktat mot de systemtjänster som upprätthåller funktionerna, men upprätthållandet kan också ha lagts ut på en aktör som egentligen inte producerar tjänsterna utan exempelvis populär programvara som det system som upprätthåller en samhällsviktig funktion stöder sig på. I punkten nämns också separat informationsmaterial kopplade till 1–6 punkten. Den föreslagna punkten täcker in situationer där det förekommer intrång i datamaterial som gäller kritiska funktioner och där dataintrånget kan leda till att den som utför intrånget läcker ut uppgifterna i offentligheten eller hamnar i händerna på någon som obehörigen utnyttjar dem. Informationsmaterial som gäller viktiga samhällsfunktioner innehåller mycket sekretessbelagd, konfidentiell och till fysiska personer kopplad information. När informationssäkerheten i fråga om den kränks eller hotas allvarligt måste myndigheterna ha möjlighet till smidig samverkan. Karakteristiskt för dataintrång är att de inte nödvändigtvis påverkar exempelvis tillgången till någon viktig tjänst, men däremot kan de kan ha betydande skadliga konsekvenser för andra skyddsobjekt, såsom privatlivet eller den nationella säkerheten, beroende på var dataintrånget sker.

En kränkning av informationssäkerheten eller ett hot om en sådan kränkning som direkt eller indirekt påverkar de nämnda vitala samhällsfunktionerna riskerar att ha omfattande konsekvenser för hela samhället, i synnerhet om verkningarna av kränkningen samtidigt berör fler än ett område. På grund av långtgående inbördes beroendeförhållanden kan konsekvenserna sträcka sig längre än det egentliga föremålet för attacken. En avgörande funktion med avseende på sådana beroendeförhållanden är exempelvis elproduktionen, eldistributionen eller kommunikationsnäten. Konsekvenserna kan gälla en eller flera funktioner. Även om konsekvenserna för en enskild samhällsfunktion inte i sig är allvarliga, kan det ändå uppkomma allvarliga skadliga konsekvenser när verkningarna på flera funktioner samverkar.

Tröskeln måste vara relativt hör när det gäller att avvika från sekretessbestämmelserna för informationsutbyte och begränsningarna av utlämnande av uppgifter enligt förslaget. Syftet med de gällande bestämmelserna om begränsning av informationsutbytet är i princip att garantera det grundlagsfästa skyddet för privatlivet och för förtroliga meddelanden, och det kan anses motiverat att avvika från det endast i ytterst exceptionella situationer. Även företag kan betrakta uppgifter om kränkningar av deras informationssäkerhet som känsliga, och uppgifterna kan också vara sekretessbelagda.

Beslutet om att tillämpa lagstiftningen ska fattas av någon av de i 1 mom. nämnda myndigheter med relevant information som har fått kännedom om en grundad misstanke om en kränkning av informationssäkerheten eller ett hot om en kränkning som uppfyller kriterierna i momentet. Det kan också hända att en myndighet i samband med sedvanligt samarbete och informationsutbyte kan kombinera uppgifter från olika källor och därmed komma till slutsatsen att det är fråga om en situation som avses i 1 mom. Myndigheterna kan också komma fram till den slutsatsen tillsammans genom sedvanligt samarbete.

I det föreslagna *2 mom.* preciseras uppgifternas användningsändamål. En begränsning att använda uppgifterna gäller bara uppgifter vars utlämnande är förenat med begränsningar eller sekretessplikt och i fråga om vilka det föreslås möjlighet till avvikelse i 1 mom. Med andra ord är avsikten inte att begränsa användningen i fråga om de uppgifter som får lämnas ut även under andra omständigheter utan begränsningar av användningsändamålet. Uppgifterna får användas

för att utreda eller förebygga kränkningar eller allvarliga hot om kränkningar av informationssäkerheten eller för att undanröja deras verkningar. I praktiken ska uppgifterna primärt användas för att utreda den kränkning eller det hot som lett till att myndigheterna lämnat ut uppgifter till varandra. Uppgifterna får emellertid också användas för att upptäcka sådana kränkningar och därigenom förebygga nya incidenter. På så sätt gör momentet det möjligt att exempelvis använda uppgifterna för att med hjälp av systemet Havaro, som Transport- och kommunikationsverket driver, identifiera senare sådana kränkningar av eller hot om kränkningar av informationssäkerheten som utnyttjar samma sårbarhet eller ledningsserver. Uppgifterna får också användas som grund för inriktningen av exempelvis polisens, skyddspolisens och Försvarsmaktens åtgärder i samband med inhämtande av teleinformation och för de krav som gäller för sådana åtgärder. Det är dock i och för sig en domstol som svara för att godkänna åtgärderna.

Enligt det föreslagna 2 mom. ska uppgifter som är onödiga för att förebygga eller utreda kränkningar eller för att undanröja deras verkningar raderas. På utplåning av uppgifter tillämpas i övrigt vad som i 316 § 4 mom. i lagen om tjänster inom elektronisk kommunikation föreskrivs om utplåning av uppgifter.

I det föreslagna *3 mom.* föreskrivs det om begränsningar i användningen och vidarelämnande av uppgifter. Den som lämnar ut uppgifterna ska i samband med utlämnandet meddela om användningen av uppgifterna är förenad med begränsningar i fråga om användningsändamål, vidarelämnande eller återsändande. Det kan till exempel vara fråga om en inskränkning i rätten till insyn i personuppgifter enligt 42 § i lagen om behandling av personuppgifter i polisens verksamhet eller 25 § i lagen om behandling av personuppgifter inom Försvarsmakten. Syftet med dessa bestämmelser är att säkra brottsutredningar, och det föreslagna 3 mom. utsträcker dessa inskränkningar också till andra myndigheter. Motsvarande inskränkningar kan också gälla exempelvis vidarelämnande av uppgifter som myndigheternas internationella partner lämnat ut eller avgränsning av användningsändamålet.

### 7.2 Lagen om behandling av personuppgifter inom Försvarsmakten

**29 §** *Rätt att lämna ut personuppgifter för fullgörande av lagstadgade uppgifter*. Det föreslås att 1 mom. 18 punkten ändras så att det i fråga om uppgifterna för Cybersäker-hetscentret vid Transport- och kommunikationsverket också hänvisas till dess särskilda uppgifter enligt lagen om tjänster inom elektronisk kommunikation. Dessutom föreslås det att ordet ”Cybersäkerhetscentret” utgår, eftersom särskilda uppgifter enligt lagen om tjänster inom elektronisk kommunikation vid Transport- och kommunikationsverket också utförs av andra inom verket än Cybersäkerhetscentret.

Särskilda uppgifter enligt 304 § 1, 7, 9 och 10 punkten i lagen om tjänster inom elektronisk kommunikation är främjande av den elektroniska kommunikationens funktion, störningsfrihet och trygghet, insamling av information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster mervärdestjänster och informationssystem samt om fel och störningar i kommunikationsnät och kommunikationstjänster. Till dessa uppgifter hör dessutom utredning av orsakerna till störningar av radiokommunikation samt till störningar som en radioutrustning eller teleterminalutrustning orsakar kommunikationsnät, radioutrustningar, teleterminalutrustningar eller elanläggningar samt utredning av kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem.

Myndigheterna behöver utbyta information med varandra när de utför uppgifter som gäller cyberstörningar. Detta beskrivs ovan i motiveringen till 319 a §. Den föreslagna ändringen kompletterar andra bestämmelser om informationsutbyte mellan Försvarsmakten och Transport- och

kommunikationsverket. Det är värt att notera att regleringen endast gäller personuppgifter och att det inte går att lämna ut uppgifter som omfattas av skyddet för förtroliga meddelanden med stöd av regleringen utan särskild grund för behandling av dessa uppgifter.

### 7.3 Lagen om behandling av personuppgifter i polisens verksamhet

**22 §** *Övrigt utlämnande av personuppgifter till myndigheter.* Enligt förslaget ska polisen i fortsättningen på begäran eller på eget initiativ få lämna ut personuppgifter till Transport- och kommunikationsverket också för skötseln av uppgifter enligt lagen om tjänster inom elektronisk kommunikation på samma sätt som Försvarsmakten ovan föreslås få rätt att lämna ut personuppgifter till Transport- och kommunikationsverket. Också hittills har uppgifter kunnat lämnas ut med stöd av 22 § 3 mom., enligt vilket polisen av grundad anledning trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd till en myndighet får lämna ut personuppgifter som är nödvändiga för att utföra en uppgift som i lag föreskrivits för myndigheten. Förslaget bidrar till att förtydliga bestämmelserna om informationsutbyte mellan polisen och Transport- och kommunikationsverket.

## 8 Ikraftträdande

Det föreslås att lagarna träder i kraft den 1 februari 2023.

## 9 Verkställighet och uppföljning

Avsikten är att i samband med att propositionen verkställs utförligt informera relevanta myndigheter med avseende på informationssäkerheten om innehållet i den nya lagstiftningen. Nyckelmyndigheterna har redan under beredningen övat tillämpningen av bestämmelserna och deltagit intensivt i beredningen. Uppföljning av hur lagstiftningen fungerar sker genom fallspecifika analyser vid praktisk tillämpning.

## 10 Förhållande till andra propositioner

Lagförslagen har kopplingar till två andra aktuella ändringar av lagen om tjänster inom elektronisk kommunikation. Regeringens proposition med förslag till med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation och av 3 § i lagen om Transport och kommunikationsverket (RP 170/2022 rd) har lämnats till riksdagen och gäller en offentligt reglerade tjänst inom ramen för ett satellitnavigeringssystem. Efter denna proposition kommer dessutom en proposition att överlämnas med förslag till lag om ändring av lagen om tjänster inom elektronisk kommunikation, som gäller skyldigheten att distribuera radio- och tv-program. Förslagen gäller inte samma paragrafer.

## 11 Förhållande till grundlagen samt lagstiftningsordning

Den föreslagna lagstiftningen innehåller förslag som bör granskas med avseende på grundlagen. Det gäller bestämmelserna om handräckning i förhållande till grundlagens 2 § 3 mom. om att all utövning av offentlig makt ska bygga på lag och förslagen som gäller utbyte av information i förhållande till 10 § om skydd för privatlivet och för förtroliga meddelanden. Förslaget bör också granskas med avseende på offentlighetsprincipen för myndigheternas verksamhet enligt 12 § 2 mom. i grundlagen.

### 11.1 Handräckning

Den föreslagna 309 § gäller handräckning som polisen, skyddspolisen och Försvarsmakten lämnar Transport- och kommunikationsverket för att förebygga och utreda betydande kränkningar av informationssäkerheten och undanröja deras verkningar. Bestämmelser om handräckning är av betydelse med avseende på rättsstatsprincipen i grundlagen. Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag och lag noggrant iakttas i all offentlig verksamhet. Premissen är att den som utövar offentlig makt alltid ska ha en behörighetsgrund som i sista hand återgår på en av riksdagen stiftad lag. Regleringen av befogenheter är vanligen relevant också i förhållande till de i grundlagen inskrivna grundläggande fri- och rättigheterna (GrUU 51/2006 rd, s. 2/I). De föreslagna bestämmelserna om handräckning är relevanta också med avseende på det i grundlagen garanterade skyddet för privatlivet och för förtroliga meddelanden.

Handräckningen gäller Transport- och kommunikationsverkets verksamhet och utförande av dess lagfästa uppgifter. Transport- och kommunikationsverket ska kunna begära handräckning av polisen, skyddspolisen eller Försvarsmakten så att den myndighet som lämnar handräckning använder sin kapacitet till att utföra en uppgift som hör till Cybersäkerhetscentret. Förslaget skapar inga nya uppgifter eller befogenheter för centret, utan det är fråga om utförande av Transport- och kommunikationsverkets uppgift enligt 304 § i lagen om tjänster inom elektronisk kommunikation, i synnerhet dess 10 punkt. Handräckning ska kunna begäras och lämnas endast vid sådan betydande kränkning av informationssäkerheten där intresset att utreda och avvärja kränkningen är större än vid vanliga kränkningar av informationssäkerheten. Handräckningen ska gälla situationer med betydande kränkningar av informationssäkerheten och även allvarliga hot om sådana kränkningar. Med allvarliga hot kan på det sätt som närmare framgår av specalmotiveringen i princip avses sådana allvarliga och omfattande systemsårbarheter som, om de exploateras, kan leda till allvarliga konsekvenser för det allmännas beslutsförmåga, samhällets kritiska infrastruktur, den allmänna ordningen eller säkerheten. Formuleringen om allvarligt hot bör enligt motiven tolkas restriktivt och med beaktande av verkningarna av att sårbarheten exploateras.

Någon form av hotrelaterade bestämmelser om handräckning ingår i och för sig också i lagen om Försvarsmaktens handräckning till polisen (342/2022), som har stiftats med grundlagsutskottets medverkan. Regleringen gäller handräckning bland annat att förhindra och avbryta ett brott som medför allvarlig fara för människors liv eller hälsa.

Grundlagsutskottet har i sin utlåtandepraxis konstaterat att en myndighets verksamhet inte kan vara uppbyggd på en handräckningsinstitution (GrUU 3/2022 rd, s. 2). Den föreslagna regleringen står inte i strid med denna princip, utan det är på motsvarande sätt som tidigare fråga om ett exceptionellt arrangemang som ska utnyttjas först om Transport- och kommunikationsverkets egna resurser inte är tillräckliga för att sköta dess lagstadgade uppgifter och andra myndigheter har den kompetens och andra resurser som behövs för att ge stöd i denna uppgift. De resurser och den kapacitet som det är fråga när handräckning för att utföra uppgifterna begärs och lämnas är i synnerhet it-resurser och it-kapacitet. Handräckning handlar om att utnyttja myndigheternas gemensamma förmågor, om Transport- och kommunikationsverket undantagsvis inte med egna resurser klarar av sina föreskrivna uppgifter, exempelvis vid en synnerligen omfattande eller exceptionellt allvarlig cyberattack.

I samband med förslag om handräckning har förvaltningsutskottet lyft fram att enbart bestämmelser om lämnande av handräckning till en annan myndighet ännu inte ger uttryck för behörighet att lämna handräckning, utan det ska i lagstiftningen finnas antingen en mer specifik eller en mer allmän befogenhet att ge handräckning (FvUU 29/2020 rd, s. 7). Förslaget inskränker

handräckningen till situationer där informationssäkerheten kränks eller allvarligt hotar att kränkas, och samtidigt har arten av handräckning begränsats till experthjälp, utrustning, lokaler och anordningar.

När det gäller handräckning har grundlagsutskottet fäst uppmärksamhet vid att handräckningen ska grunda sig på myndigheternas behörighet att sköta en viss uppgift (GrUU 10/2005 rd, s. 2/II). När det gäller polisen och skyddspolisen grundar sig handräckningen på polisens grundläggande uppgifter i fråga om rätts- och samhällsordningen och den nationella säkerheten samt i synnerhet i fråga om förebyggande, avslöjande och utredning av brott. Polisen har flera befogenheter i anslutning till nätmiljön exempelvis i 5 och 5 a kap. i polislagen. I fråga om försvarsmakten är det fråga om tryggande av Finlands territoriella integritet i anslutning till dess grundläggande uppgift och även om handräckning enligt 2 § i lagen om försvarsmakten bland annat för att skydda samhället. Handräckning anses i förslaget inte innefatta förslag som gäller utövande av särskilda befogenheter, utan det är snarare fråga om att ge myndigheter som agerar i en motsvarande miljö med stöd av sina befogenheter tillgång till resurser, såsom kompetens och utrustning. Förslaget har till denna del inte bedömts stå i strid med 2 § i grundlagen.

Enligt förslaget är det i fortsättningen Transport- och kommunikationsverket självt som fattar beslut i fråga om handräckning i stället för kommunikationsministeriet. Förslaget bygger på att en myndighet fattar sina egna beslut om ärenden som hör till dess behörighet, och ministeriet fyller ingen särskild funktion i det sammanhanget. Grundlagsutskottet har i sin utlåtandepraxis tagit ställning till besluten om att lämna handräckning. Vid handräckning där Försvarsmakten anlitas för användning av maktmedel har utskottet ansett det viktigt att handräckningsbesluten också i brådskande fall fattas i ett ministerium som leds av en minister som ansvarar inför riksdagen, om det på grund av brådska inte är möjligt att fatta beslutet vid statsrådets allmänna sammanträde (GrUU 23/2005 rd, s. 5 och GrUU 3/2022 rd, s. 4–5). Utskottet har emellertid begränsat dessa handräckningsfrågor som kräver beslutsfattande på hög nivå till situationer där maktmedel används. Det nu aktuella förslaget står inte i strid med denna princip, eftersom den handräckning som Transport- och kommunikationsverket lämnar består av experthjälp och andra resurser och handräckningen inte förutsätter användning av maktmedel. Också besluten om att Försvarsmakten lämnar polisen annan än krävande handräckning fattas av huvudstaben eller av Arméstaben, Marinstaben eller Flygstaben.

Förslagen om handräckning anses med stöd av vad som anförs ovan inte stå i strid med grundlagen.

### 11.2 Informationsutbyte mellan myndigheter och informationens användningsändamål

#### 11.2.1 Konfidentiell kommunikation

Kärnfrågan avseende de grundläggande fri- och rättigheterna i propositionen gäller skyddet för privatlivet enligt 10 § i grundlagen, särskilt skyddet för förtroliga meddelanden enligt dess 2 mom. Enligt artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna har var och en rätt till respekt för sina kommunikationer, och artikel 8 i stadgan gäller rätten till skydd av personuppgifter. Dessutom ska personuppgifter behandlas för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Skyddet för förtroliga meddelanden garanteras också i artikel 8 i Europakonventionen (FördrS 63/1999), enligt vilken var och en har rätt till skydd för sin korrespondens. Offentliga myndigheter får inte ingripa i denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den 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. Grundlagsutskottet har slagit fast

att skyddet för privatlivet enligt 10 § i grundlagen bygger på att den enskilde har rätt att leva sitt eget liv utan godtycklig eller ogrundad inblandning av myndigheter och utomstående (GrUU 53/2005 rd, s. 2, GrUU 36/2002 rd, s. 5/II, och GrUU 9/2004 rd, s. 5/II).

I 10 § 4 mom. i grundlagen ingår särskilda begränsningsklausuler där den som stiftar vanlig lag bemyndigas att begränsa en grundläggande fri- eller rättighet, men samtidigt uppställs ytterligare kriterier som inskränker lagstiftarens prövningsrätt. Syftet med sådana kvalificerade lagförbehållen är att så noggrant och strikt som möjligt bestämma vilka möjligheter till inskränkningar lagstiftaren i samband med en vanlig lag har för att det inte genom grundlag medges en vidare befogenhet att inskränka en grundläggande fri- och rättighet än vad som är absolut nödvändigt (GrUB 25/1994 rd, s. 6). I lagförbehållet i 10 § 4 mom. i grundlagen nämns delvis samma villkor som i de allmänna villkoren för begränsning av grundläggande fri- och rättigheter. Dessa är kravet på bestämmelser i lag och begränsningens nödvändighet. De allmänna begränsningsvillkoren tillämpas som komplement till lagförbehållet. I förslaget är det fråga om en sådan nödvändig begränsning som avses i 10 § 4 mom. i grundlagen för att garantera individens eller samhällets säkerhet men också på grund av ett allvarligt hot mot den nationella säkerheten.

Propositionen innebär ett förslag till undantag från sekretessbestämmelserna och inskränkningarna när det gäller att lämna ut information. Polisen, skyddspolisen, Försvarsmakten och Transport- och kommunikationsverket ska trots dessa få lämna ut upp-gifter till varandra vid betydande kränkningar av informationssäkerheten eller vid allvarliga hot om sådana. Utlämnandet av information ska i praktiken gälla i synnerhet utlämnande av uppgifter som gäller kommunikation. Begränsningar i utlämnandet av dessa uppgifter finns särskilt i den lagstiftning som gäller Transport- och kommunikationsverket. Utlämnandet ska också gälla uppgifter som betraktas som personuppgifter. Förslaget utvidgar således de lägen där uppgifter kan lämnas ut i enskilda situationer.

Allmänt taget begränsar förslaget i första hand skyddet för förtroliga meddelanden vid informationsutbyte. Grunden för informationsutbytet är å andra sidan bland annat skyddet för konfidentiell kommunikation, vilket innebär att det skyddet indirekt främjas genom begränsningar i enskilda fall. Den inverkan på de grundläggande fri- och rättigheterna som skyddet för förtroliga meddelanden har blir således en indirekt följd av de åtgärder som myndigheterna vidtar när de utreder och förebygger kränkningar av informationssäkerheten och undanröjer deras verkningar.

I anslutning till skyddet för förtroliga meddelanden har grundlagsutskottet påpekat att identifieringsuppgifter, som senare börjat kallas förmedlingsuppgifter, inte omfattas av kärnområdet i den grundläggande fri- och rättigheten för sekretess i fråga om konfidentiella meddelanden och därför ansett det möjligt att rätten att få identifieringsuppgifter inte binds till vissa typer av brott, om bestämmelserna i övrigt uppfyller de allmänna kraven på begränsningar av de grundläggande fri- och rättigheterna (GrUU 7/1997 rd, s. 2/I, och GrUU 26/2001 rd, s. 3/II). I förslaget är det utöver förmedlingsuppgifter också fråga om exempelvis sådana uppgifter om innehållet i ett meddelande där det finns särskilda sekretessplikter och begränsningar som gäller deras utlämnande.

Grundlagsutskottet har ansett att olika åtgärder för att garantera informationssäkerheten är godtagbara med avseende på grundlagen, inklusive ingrepp i innehållet i förtroliga meddelanden under vissa förutsättningar som gäller allvarlig brottsmisstanke, när regleringen garanterar dem som kommunikationen gäller fungerande och säkra datanät och på så sätt skapar förutsättningar för yttrandefrihet och skydd för förtroliga meddelanden på nätet. De omständigheter som på detta sätt syftar till att främja och tillgodose de grund-läggande fri- och rättigheterna har ansetts

vara godtagbara och vägande skäl för begränsningar i konfidentiell kommunikation på nätet. Med avseende på proportionalitet har åtgärderna ansetts vara motiverade, om de är nödvändiga för att trygga nät- eller kommunikationstjänsterna eller kommunikationsmöjligheterna för den som tar emot meddelandet. Dessutom har kommunikations om gäller sabotageprogram inte ansetts höra till kärnområdet för skyddet av förtroliga meddelanden, eftersom det inte är fråga om ett sådant meddelande till eller från en person där förtroligheten i fråga om innehållet kan anses stå i centrum för det grundlagsfästa skyddet för förtroliga meddelanden (GrUU 9/2004 rd, s. 4). Utifrån detta kan också informationsutbyte mellan myndigheter på det sätt som nu föreslås anses vara möjligt.

Avsikten är att med stöd av förslaget göra det möjligt att i lägen där informationssäkerheten kränks eller allvarligt hotar att kränkas lämna ut förmedlingsuppgifter och uppgifter om innehållet i meddelanden, men också andra nödvändiga uppgifter, mellan myndigheter. Med tanke på skyddet för förtroliga meddelanden och privatlivet innehåller förslaget därför flera inskränkningar. Utbytet ska vara möjligt endast om det med avseende på konsekvenserna för samhällets kärnfunktioner är fråga om en särskilt betydande kränkning av informationssäkerheten som i praktiken alltid uppfyller rekvisitet för åtminstone ett av de informationssäkerhetsbrott som räknas upp i 316 § 2 mom. i lagen om tjänster inom elektronisk kommunikation eller för exempelvis spioneribrott. I fråga om hot om en kränkning av informationssäkerheten redogörs det i motiveringen ovan för sådana exceptionellt allvarliga hotsituationer där verkningarna motsvarar en kränkning av informationssäkerheten enligt förslaget om hotet realiseras. Dessutom har betydelsen av sannolikheten för att hotet realiseras understrukits. Tolkningen av vad som är ett hot ska enligt förslaget vara restriktiv eftersom analysen då blir mer osäker. Utlämnandet av uppgifter är knutet till nödvändighetskriteriet på det sätt som grundlagsutskottets tolkningspraxis förutsätter. Grundlagsutskottet har fäst uppmärksamhet vid att om det inte går att i lagen på ett uttömmande sätt specificera innehållet i de uppgifter som lämnas ut, ska det i lagstiftningen ingå ett krav på att uppgifterna är nödvändiga för ett visst syfte (GrUU 62/2010 rd, s. 4/1 och de utlåtanden som nämns där). Enligt förslaget är ett sådant syfte att utreda, förebygga eller undanröja verkningarna av betydande kränkningar av informationssäkerheten.

Förslaget är i sig inte direkt knutet till rekvisitet för vissa brott, även om något av rekvisiten för ett informations- eller kommunikationsbrott eller exempelvis spioneribrott i praktiken uppfylls i situationer med betydande kränkningar av informationssäkerheten. Att knyta tillämpningen av bestämmelsen till vissa rekvisit skulle vara svårt särskilt när det gäller att reagera på hot.

### 11.2.2 Sekretess samt begränsningar när det gäller att lämna ut uppgifter

Grundlagsutskottet har understrukit att det vid en särskiljning mellan behövlighet respektive nödvändighet att få eller lämna ut uppgifter är fråga inte bara om omfattningen av innehållet i uppgifterna utan också om att de intressen som berättigar till sådant informationsutbyte som går före sekretessbestämmelserna åsidosätter de grunder och intressen som skyddas av sekretessen. Ju mer generella bestämmelserna om rätten till information är, desto större är risken för att sådana intressen kan åsidosättas per automatik. Utlämnandet av uppgifter bör enligt utskottet bindas till nödvändighetskravet (GrUU 35/2018 rd, s. 27). Avsikten med förslaget är att skydda samhällets förmåga att fungera och de kritiska samhällsfunktionerna mot allvarliga kränkningar av informationssäkerheten, som i värsta fall kan ha allvarliga konsekvenser för samhället. Med tanke på samhällets säkerhet kan det således anses att intressena i dessa enskilda situationer överskrider de sekretessintressen som skyddas genom sekretessbestämmelserna. Om en kränkning av informationssäkerheten realiseras fullt ut är det dessutom möjligt att konsekvenserna för skyddet för förtroliga meddelanden är betydligt skadligare och berör flera personer än ett informationsutbyte mellan myndigheter i ett enskilt fall. Detta kan vara fallet till exempel i samband med omfattande dataintrång.

### 11.2.3 Förhållande till underrättelseverksamhet och brottsbekämpning

Eftersom sådan information i Transport- och kommunikationsverket besittning som är sekretessbelagd och åtnjuter skydd för förtroliga meddelanden, vid ömsesidigt informationsutbyte kan lämnas ut till skyddspolisen och Försvarsmakten och vid behov också mellan dessa, behöver förslagets granskas i förhållande till underrättelseverksamheten och tillhörande frågor om de grundläggande fri- och rättigheterna, särskilt med avseende på konfidentiell kommunikation. Det är i sig fråga om informationsutbyte i en väl avgränsad situation som gäller ett enskilt fall och inte om en bred kanal för generellt informationsutbyte. Grundlagsutskottet har i fråga om detta bestämt att en ändring av grundlagen inte möjliggör en allmän, oriktad och heltäckande övervakning av datatrafiken i underrättelseverksamheten (GrUB 4/2018 rd, s. 8). Också EU-domstolen har i sin praxis slagit fast att informationsinhämtning ska vara tillräckligt riktad och specificerad. Enligt EU-domstolen kräver skyddet av den grundläggande rätten till respekt för privatlivet under alla omständigheter att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt (dom digital Rights Ireland m.fl., punkt 52 och där angiven rättspraxis). Också grundlagsutskottet har fört fram sin ståndpunkt om inriktning och avgränsning när det gäller underrättelseverksamhet (GrUB 4/2018 rd, s. 7–8). Förslaget anses inte stå i strid med dessa specialvillkor för inriktning och avgränsning av informationsinhämtningen.

Grundlagsutskottet har i samband med den ändring av grundlagens 10 § som gäller underrättelselagarna framfört de viktigaste grunder som måste beaktas vid bedömningen av sådan militär verksamhet eller annan verksamhet som allvarligt hotar den nationella säkerheten enligt 10 § 4 mom. i grundlagen som utgör grund för begränsning av hemligheten i fråga om förtroliga meddelanden. Utskottet har lyft fram starka rättssäkerhetsgarantier, bred och effektiv tillsyn över utövningen av befogenheterna till underrättelseinhämtning och lämpligt avgränsad tillämpning. Det rör sig om en exceptionell begränsningsgrund som inte bygger på att verksamheten ska

vara brottslig och som således blir tillämplig också i fall där det inte går att peka på någon konkret och specificerad misstanke om brott varken i informationsinhämtningsfasen eller i övrigt (GrUB 4/2018 rd, s. 8).

Även om det inte i sig är fråga om en metod för inhämtande av information inom underrättelseverksamheten, kan den information som utbytts i en sådan situation som avses i förslaget vara sådan att underrättelsemyndigheten i andra situationer ansöker om tillstånd hos domstolen för att få den. Transport- och kommunikationsverkets uppgift innebär att verket har tillgång till och i vissa situationer innehar sådana uppgifter som underrättelsemyndigheter och inte heller brottsbekämpande myndigheter har direkt tillgång till utan tillstånd av domstol. Förslaget som helhet gäller avgränsade och i lag angivna fall, och de innebär inte att regleringen skulle utgöra något betydande undantag från de principer som gäller för underrättelseinhämtning. Avsikten har varit att noggrant avgränsa informationens användningsändamål på så sätt att den kan användas bara för att utreda, förebygga och undanröja verkningarna av kränkningar av informationssäkerheten. Informationen kan således också användas särskilt för förebyggande verksamhet i enlighet med myndigheternas lagstadgade uppgifter också i andra situationer än de som lett till att in-formationen lämnats ut. I fråga om garantierna för rättsmedel fyller avgränsningen av informationens användningsändamål en viktig funktion. Med tanke på helheten är det dock ändamålsenligt att information om allvarliga situationer kan användas för att främja den nationella säkerheten, och därför ska informationen kunna användas för att rikta in underrättelseverksamheten, och då garanteras rättssäkerheten dels av domstol, dels genom förebyggande åtgärder.

När information lämnas ut till polisen och Försvarsmakten måste man utöver underrättelseverksamheten också granska hur informationsutbytet förhåller sig till brottsbekämpningen, för det

första med avseende på att det i fråga om informationsutbyte har föreskrivits om en särskild s.k. brandvägg mellan underrättelseverksamheten och brottsbekämpningen. Med brandmur avses att uppgifter som inhämtats genom underrättelsebefogenheter inte får överföras till en förundersökningsmyndighet utan att de lagstadgade kriterierna är uppfyllda. Utlämnande av sådana uppgifter för brottsbekämpning är möjligt efter prövning i fråga om vissa allvarliga brott, men samtidigt obligatoriskt i fråga om särskilt allvarliga brott. Ett nyckelelement som styr prövningen är hur utlämnandet av uppgifter påverkar den nationella säkerheten. Grundlagsutskottet har ansett det vara viktigt att säkerställa att bestämmelserna om utbyte av information som erhållits genom befogenheter till underrättelseinhämtning inte öppnar upp för möjligheter att kringgå bestämmelserna om hemliga metoder för inhämtande av information i polislagen och om användning av hemliga tvångsmedel i tvångsmedelslagen, där tröskeln för tillämpning i praktiken är högre (GrUU 35/2018 rd, s. 21–22). Eftersom myndigheterna i de situationer som avses i förslaget inbördes kan lämna ut uppgifter till varandra, finns det en möjlighet att information som erhållits genom en metod för underrättelseinhämtning i samband med informationsutbytet också får lämnas ut till en förundersökningsmyndighet.

Både i lagen om militär underrättelseverksamhet och i polislagens 5 a kap. om civil underrättelseinhämtning finns bestämmelser om utlämnande till en förundersökningsmyndighet av information som inhämtats genom en metod för underrättelseinhämtning. Underrättelsemyndigheterna har rätt att anmäla endast sådana genom en metod för underrättelseinhämtning avslöjade brott där det föreskrivna strängaste straffet är fängelse i minst tre år. Allvarliga brott som kan förhindras ska utan dröjsmål anmälas till förundersökningsmyndigheten, och rätt att anmäla föreligger för brott där det föreskrivna strängaste straffet är fängelse i två år. Ett villkor för fakultativ anmälan av brott är att anmälan bedöms vara av synnerlig vikt för utredningen av ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst tre år. I de situationer som avses i förslaget uppfylls ofta strafflagens rekvisit för exempelvis grov systemstörning och grovt dataintrång, och då är det möjligt att lämna ut information även utan undantagsbestämmelser också i fråga om information som lämnas ut för förundersökning. Samma läge föreligger exempelvis i fråga om spioneribrott, röjande av statshemlighet och olovlig underrättelseverksamhet, och i fråga om dessa är utlämnande av information för brottsbekämpning enligt lag delvis till och med obligatoriskt. I dessa delar står förslaget inte i strid med grundlagsutskottets ståndpunkt ovan. I fråga om ringare brott kan det i vissa situationer uppkomma ett läge där förundersökningsmyndigheten får kännedom om information om ett sådant brott via underrättelseverksamheten. Straffet för exempelvis systemstörning eller dataintrång är fängelse i högst två år. Med andra ord överskrids inte den ovan relaterade tröskeln för utlämnande av information, såvida inte brottet fortfarande går att förhindra. I dessa fall kan en betydande kränkning av informationssäkerheten enligt förslaget komma i fråga när åtgärder som utgör ringare brott genomförs på flera ställen samtidigt, varvid effekten kan flerdubblas. Också här måste det avvägas huruvida det är fråga om en grov gärningsform av brotten, vilket i så fall medger utlämnande av information för brottsbekämpning. Utifrån detta kan det anses att förslaget inte i dessa delar medför något betydande undantag från inskränkningarna när det gäller att lämna ut uppgifter.

En annan aspekt i fråga om brottsbekämpning gäller utlämnande av sådan information för brottsbekämpning som Transport- och kommunikationsverket fått. Transport- och kommunikationsverket har till uppgift att säkerställa konfidentialitet vid kommunikationen exempelvis genom sitt Cybersäkerhetscenter. Verket får information genom sin egen verksamhet och genom frivilliga anmälningar till Cybersäkerhetscentret, och på detta sätt får det kännedom också om information som myndigheterna för brottsbekämpning och underrättelseverksamhet måste ansöka om tillstånd hos domstol för att få, vilket beror på att rättssäkerheten måste tillgodoses. Det är delvis därför som det har föreskrivits särskilda sekretessplikter och inskränkningar för utlämnande av information som verket disponerar över. Meddelandets innehåll, förmedlingsuppgifter och lokaliseringsuppgifter får i princip lämnas ut till andra myndigheter endast när

myndigheten själv har råkat ut för eller hotas av en kränkning av informationssäkerheten. Förslaget utgör ett undantag från denna princip i lägen där myndigheterna lämnar ut information sinsemellan. Utifrån det som sägs ovan kan det slås fast att den nytta som undantaget medför med avseende på konfidentialitet vid kommunikationen stor i förhållande till orsakad olägenhet. Samtidigt bör det påpekas att syftet med inskränkning av informationens användningsändamål är att säkerställa att rättsmedel är tillgängliga även i fortsättningen.

### 11.2.4 Bedömning av villkoren för inskränkning av de grundläggande fri- och rättigheterna

Sett till de allmänna villkoren för inskränkningar av de grundläggande fri- och rättigheterna och begränsningsvillkoret i 10 § 4 mom. i grundlagen uppfyller förslaget kravet på bestämmelser i lag. När det gäller exakthet och noggrann avgränsning är det på det hela taget en utmaning att i alla delar begränsa informationsutbytet om kränkningar av informationssäkerheten. Begreppet kränkning eller allvarligt hot om kränkning av informationssäkerheten är omfattande och täcker in många olika gärningsformer. Dessutom utvecklas tillvägagångssätten hela tiden i takt med att tekniken utvecklas. Men också föremålet för kränkningen eller hotet spelar en viss roll. Kränkningen kan riktas mot en enskild aktör eller med större omfång mot flera tusen privatpersoner och därmed vara betydande på det sätt som avses i förslaget. En mycket stor krets av privatpersoner, företag, organisationer eller myndigheter kan bli föremål för dessa kränkningar. Denna mångfald innebär att det ytterst svårt att i detalj avgränsa regleringen när man vill att myndigheterna ska kunna vidta åtgärder i alla dessa situationer.

Begreppen nationell säkerhet, försvaret och det allmännas beslutsförmåga är omfattande till sitt innehåll och i viss mån ospecificerade. Den mångfald av situationer som framgår av föregående stycke innebär vidare att det inte heller varit möjligt att ge en uttömmande förteckning över de uppgifter som kan utbytas. Därför har strävan varit att göra andra avgränsningar utifrån vilka förslaget kan anses uppfylla kravet på exakthet och noggrann avgränsning. Även om konsekvenserna av en kränkning av informationssäkerheten eller ett hot om en sådan kränkning i vissa delar är vagt definierade, medför tillämpningen av förslaget i praktiken inga andra rättigheter än sådana som gäller nödvändigt informationsutbyte. Förslaget skiljer sig i detta avseende avsevärt från exempelvis det som står i beredskapslagen, eftersom förslagets rättsverkningar är betydligt mer begränsade. Dessutom upphör heller inte sekretessen när myndigheterna utbyter information. I förslaget har informationsutbytet begränsats till vissa myndigheter, informationen har inskränkts till att gälla endast nödvändiga uppgifter och uppgifterna får användas bara för att utreda, förebygga eller undanröja verkningarna av kränkningar av informationssäkerheten. Dessutom krävs det att konsekvenserna är allvarliga. I fråga om allvarliga hot ska tolkningen dessutom vara restriktiv och det ska beaktas hur sannolikt det är att konsekvenserna realiseras, och då ska sannolikheten vara stor. I dessa delar kan det bedömas att kravet på exakthet och noggrann avgränsning på det hela taget blir uppfyllt.

I fråga om personuppgifter har grundlagsutskottet i sin praxis i förhållande till tidigare kriterier för informationsutbyte preciserat att sekretessbelagda personuppgifter inte får lämnas ut ens med stöd av nödvändighetskriteriet, om rätten att få uppgifter annars har definierats på ett vagt och ospecificerat sätt (GrUU 19/2012 rd, s. 3–4, och de utlåtanden som nämns där). Informationsutbyte i enlighet med förslaget har till denna del knutits till nödvändighetskriteriet, och samtidigt anges det också vilka myndigheter som får utbyta information med varandra. Därför kan förslaget inte i detta avseende anses vara konstitutionellt problematiskt.

Med avseende på hur godtagbart det är att inskränka skyddet för förtroliga meddelanden anses det vara av särskild betydelse om det finns ett väsentligt behov av att trygga centrala samhällsfunktioner. Också i 10 § 4 mom. i grundlagen förutsätts det att begränsningar i meddelandehemligheten ska vara nödvändiga bland annat vid utredning av brott som äventyrar individens

eller samhällets säkerhet eller hemfriden eller för att inhämta information om sådan annan verksamhet som allvarligt hotar den nationella säkerheten. Allvarliga kränkningar av informationssäkerheten kan ha långtgående och komplexa konsekvenser för olika sektorer och på så sätt för både individens eller samhällets säkerhet och den nationella säkerheten. Kränkningar av informationssäkerheten kan försvaga skyddet för privatlivet, och samtidigt kan de också beroende på vem som utsätts för kränkningen också få konsekvenser som gäller liv och hälsa. Ur denna synvinkel har förslaget ansetts ha godtagbara grunder som uppfyller nödvändighetskravet för att be-gränsa skyddet för förtroliga meddelanden.

Med avseende på proportionalitetskravet kan rätt att lämna ut uppgifter komma i fråga endast i enskilda fall. Det anges också vad informationen får användas till, och användningsändamålet är avgränsat. Avgränsningen har ansetts står i rätt proportion till att väsentliga samhällsfunktioner ska säkerställas. Dessutom har ribban satts relativt högt när det gäller att tillämpa bestämmelserna, vilket understryker nödvändigheten i de berörda och mycket allvarliga säkerhetshotande situationerna. Då är det nödvändigt att tillämpa exceptionella rättigheter till informationsutbyte.

När det gäller tillräckliga garantier för rättssäkerheten gäller rättsmedlen i praktiken de myndighetsfunktioner med stöd av vilka information de facto samlas in. Dessa är således i synnerhet befogenheter som gäller underrättelseverksamhet och tvångsmedel inom de hemliga metoder för inhämtande av information som används i samband med behandling av personuppgifter, underrättelseverksamhet och brottsbekämpning. Enligt förslaget avses sådan information inte inbegripa möjlighet att använda den erhållna informationen för tillräknande, utan för detta ändamål ska sedvanliga metoder användas. Genom förslaget skapas inte något egentligt nytt sätt för myndigheterna att inhämta information för att sköta andra lagstadgade uppgifter, utan informationen används endast i samband med utredning av kränkningar av informationssäkerheten. Dessutom finns det till den del det är fråga om personuppgifter rättsmedel i anslutning till dataskyddet. Rättsmedlen anses till dessa delar vara tillräckliga.

Propositionen anses ligga i linje med förpliktelserna i fråga om de mänskliga rättigheterna. I detta sammanhang är Europakonventionen av särskild betydelse, såsom dess innehåll ser ut i ljuset av Europadomstolens rättspraxis. Enligt Europadomstolens rättspraxis krävs det alltid att en inskränkning av förtrolig kommunikation motiveras av ett vägande samhälleligt behov, att ingripandet och det godtagbara mål som eftersträvas står i rätt proportion till varandra och att det finns relevanta och tillräckliga skäl för inskränkningen. Dessutom måste inskränkningarna vara tillåtna enligt lag. Europadomstolens rättspraxis understryker kvaliteten på lagstiftningen, såsom exakthet, och reglering som tryggar förutsägbarheten i myndigheternas verksamhet och förhindrar maktmissbruk. Förslaget anses uppfylla dessa krav.

### 11.2.5 Dataskydd vid informationsutbyte mellan myndigheter

Enligt 10 § 1 mom. i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Grundlagsutskottet har ansett att skyddet för personuppgifter i första hand bör tillgodoses med stöd av EU:s allmänna dataskyddsförordning och den nationella lagstiftningen och vara avgränsad till vad som är nödvändigt inom ramen för det handlingsutrymme som dataskyddsförordningen medger (GrUU 14/2018 rd, s. 4–5).

Med stöd av den föreslagna 319 a § utbyts också uppgifter som anses vara personuppgifter. Myndigheternas rätt att behandla dessa uppgifter kommer nu att utvidgas uttryckligen i fråga om utlämnandet. I övrigt har de redan nu rätt att behandla uppgifterna i fråga. I förslaget är det således fråga om sådan behandling av uppgifter som avses i artikel 4 i dataskyddsförordningen

och 3 § 1 mom. 2 punkten i dataskyddslagen avseende brottmål, eftersom myndigheterna lämnar ut och sammanför uppgifter som de innehar, såsom förmedlingsuppgifter. På verksamheten hos de myndigheter som avses i förslaget eller på någon del av verksamheten tillämpas för sin del olika dataskyddsbestämmelser, vilket framgår av avsnitt 2.2.4 om nuläget. I de situationer som avses i förslaget är det således möjligt att personuppgifter vid informationsutbyte används för andra ändamål än det ursprungliga, i synnerhet om uppgifter överförs från brottsbekämpningsmyndigheterna till Transport- och kommunikationsverket eller vice versa.

Förmedlingsuppgifterna omfattas i sig av den nationella regleringen för genomförande av direktivet om integritet och elektronisk kommunikation. Sådan reglering finns särskilt i lagen om tjänster inom elektronisk kommunikation. Särskilt viktig är direktivartikel 15.1, enligt vilken medlemsstaterna genom lagstiftning får vidta åtgärder för att begränsa vissa rättigheter och skyldigheter enligt direktivet. En sådan begränsning ska vara nödvändig, lämplig och proportionell i ett demokratiskt samhälle för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem. En bedömning enligt dessa kriterier har ansetts vara analog med en bedömning enligt ovan av rätten att begränsa grundläggande fri- och rättigheter och samtidigt även med en bedömning av bestämmelserna om integritetsskydd.

Bestämmelsen möjliggör i sig utbyte av all nödvändig information, vilket inte kategoriskt utesluter möjligheten till utbyte av personuppgifter som hör till de särskilda kategorier av personuppgifter som avses i dataskyddslagen (1050/2018). Den föreslagna avgränsningen, dvs. att de uppgifter som lämnas ut ska vara nödvändiga för att utreda, förebygga eller undanröja verkningarna av en kränkning av informationssäkerheten, begränsar dock i praktiken sådant informationsutbyte främst till teoretisk nivå. Sådana uppgifter saknar betydelse för utredning av kränkningar av informationssäkerheten, och när information där sådana uppgifter eventuellt ingår behandlas med stöd av andra kriterier exempelvis i samband med behandling av material som gäller dataintrång, behöver de inte lämnas ut till en annan myndighet, utan de ska enligt bestämmelsen raderas såsom onödiga, om inte något annat följer av annan lag.

Enligt de allmänna principerna för behandling av personuppgifter i artikel 5 i dataskyddsförordningen är särskilt kraven på laglighet, korrekthet och öppenhet väsentliga. Dessutom ska personuppgifter samlas in för särskilda, uttryckligt angivna ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Bestämmelser om undantag från användningsändamålet för personuppgifter finns i artikel 6.4 i dataskyddsförordningen. Avvikelsen får enligt artikeln grunda sig på medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1. I skäl 50 till förordningen slås det fast att om behandlingen grundar sig på medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa i synnerhet viktiga mål av allmänt intresse, bör den personuppgiftsansvarige tillåtas att behandla personuppgifterna ytterligare, oavsett om detta är förenligt med ändamålen eller inte. Under alla omständigheter bör tillämpningen av principerna i förordningen, särskilt informationen till den registrerade om dessa andra ändamål och om dennes rättigheter, inbegripet rätten att göra invändningar, säkerställas.

I förslaget används det nationella handlingsutrymme som artikel 23 medger på så sätt att den föreslagna lagstiftningsåtgärden innebär en ändamålsbegränsning enligt artikel 5. De förslag som syftar till att säkerställa den nationella säkerheten och samtidigt också möjliggöra förebyggande av brott har ansetts vara nödvändiga och stå i rätt proportion till det eftersträvade skyddsintresset. Det anses finnas vägande samhälleliga skäl för att göra undantag från ändamålet när

det gäller att skydda kritiska samhällsfunktioner. Samtidigt har kravet på proportionalitet uppfyllts när en avgränsning gjorts till nödvändiga uppgifter till nödvändiga, men också genom en relativt hög tröskel för tillämpning av undantagsbestämmelsen, dvs. bara i situationer med allvarliga konsekvenser.

Utlämnande av uppgifter enligt förslaget kan i vissa situationer också ske direkt med stöd av 16 § 3 mom. i offentlighetslagen. Det är inte alltid fråga om undantag från ändamålsbegränsningen för personuppgifter, utan behandlingen kan ske med stöd av den ursprungliga behandlingsgrunden eller en behandlingsgrund som är förenlig med den. Kriteriet för behandling av personuppgifter är då utförande av en uppgift av allmänt intresse och som ett led i den personuppgiftsansvariges myndighetsutövning. I annat fall utgörs grunden för behandlingen av den föreslagna lagstiftningen, och målet av allmänt intresse enligt artikel 6.3 är att säkerställa den allmänna säkerheten vid kränkningar av informationssäkerheten. Bestämmelsen om utlämnande av information anses stå i rätt proportion till det eftersträvade målet, med beaktande av de begränsningar som nämns ovan.

### 11.3 Kommunikationsförmedlares rätt att lämna ut information till Transport- och kommunikationsverket

Också den föreslagna 316 a § är relevant med avseende på skyddet för privatlivet enligt 10 § i grundlagen. Enligt förslaget ska en kommunikationsförmedlare ha möjlighet att frivilligt lämna ut information om innehållet i elektroniska meddelanden och om förmedlingsuppgifter som gäller kränkningar av informationssäkerheten. Förslaget inskränker i någon mån konfidentialiteten vid kommunikation, eftersom det innefattar möjligheten att lämna ut information om innehållet i meddelanden. Den föreslagna informationsdelning som avser meddelandets innehåll har inte bedömts vara särskilt problematisk med avseende på kommunikationens konfidentialitet, eftersom det främst kommer att vara fråga om innehållet i meddelanden som innehåller sabotageprogram eller exempelvis orsakar kränkningar av informationssäkerheten, och då är den andra inblandade sällan ens är en fysisk person utan till exempel ett datorprogram som genererar meddelanden automatiskt. Förslaget har inte ansetts innebära någon betydande förändring när det gäller den nuvarande rätten att behandla motsvarande uppgifter, men däremot det har ansetts förbättra möjligheterna att ingripa i kränkningar av informationssäkerheten och främja skyddet för förtroliga meddelanden och privatlivet för dem som blivit utsatta för kränkningarna. Om skadliga meddelanden spärras går det exempelvis att förhindra att fysiska personer får bluffmeddelanden. Men en del av de uppgifter som lämnas ut kan också innehålla helt saklig kommunikation, och då blir inskränkningen av integritetsskyddet och kommunikationens konfidentialitet mer betydande.

För behandlingen av uppgifterna innehåller förslaget bestämmelser om de behandlingsprinciper och den sekretess som ska iakttas vid sådant utlämnande av uppgifterna som här avses. Utifrån dem är behandling tillåten endast i den omfattning som syftet kräver och på så sätt att skyddet för förtroliga meddelanden och privatlivet inte begränsas mer än nödvändigt. Bestämmelsen innehåller också krav på radering och anonymisering av uppgifter efter behandlingen, om inte något annat föreskrivs i lag. På utlämnande av uppgifter enligt bestämmelsen tillämpas sekretessen enligt 319 § och bestämmelserna om utlämnande av uppgifter i både 319 och 319 a §. I detta avseende har förslaget bedömts ligga i linje med kraven i 10 § i grundlagen.

Redan enligt gällande lagstiftning har både kommunikationsförmedlaren och Transport- och kommunikationsverket rätt att behandla de uppgifter som avses i förslaget för att sörja för informationssäkerheten. Verket har också möjlighet att begära sådan information av kommuni-

kationsförmedlaren om det upptäcker ett sådant behov. Förslaget innebär således ingen betydande förändring jämfört med nuläget, och utifrån en samlad bedömning kan det anses vara förenligt med 10 § i grundlagen.

Förslaget gäller dessutom behandling av personuppgifter, i synnerhet personuppgifter inom elektronisk kommunikation. Eftersom utlämnande av information också betraktas som behandling av personuppgifter, utgör förslaget i detta avseende en ny grund för behandling av de uppgifter som avses i paragrafen. När det gäller kommunikationsförmedlare är det fråga om uppfyllande av kravet på säkerhet i samband med behandling av uppgifter enligt artikel 4 i direktivet om integritet och elektronisk kommunikation, men eftersom utlämnande av uppgifter till Transport- och kommunikationsverket inte direkt medför någon skyldighet med stöd av den artikeln uppkommer det således i viss utsträckning en begränsning av skyddet av konfidentiell kommunikation. En begränsning är möjlig med stöd av de begränsningsgrunder som anges i artikel 15 och till denna del används det nationella handlingsutrymmet. Begränsningen är motiverad med avseende på allmän säkerhet och förebyggande av brott. Vid den senare behandlingen inom Transport- och kommunikationsverket är det fråga om behandling av personuppgifter enligt dataskyddsförordningen. Sett ur ett personuppgiftsperspektiv är det fråga om utlämnande av uppgifter till någon annan för samma eller förenliga ändamål. Behandlingen är nödvändig för ett behov enligt artikel 6 i dataskyddsförordningen för att utföra en uppgift av allmänt intresse. Nationella bestämmelser om grunder för behandling finns i 243, 247 och 272 § i lagen om tjänster inom elektronisk kommunikation i fråga om kommunikationsförmedlare och i 304, 316 och den föreslagna 316 a § i samma lag och 2 och 3 § i lagen om Transport- och kommunikationsverket (935/2018) i fråga om Transport- och kommunikationsverket. För bådas del grundar sig rätten att behandla uppgifter på bestämmelserna om att sörja för informationssäkerheten och utreda kränkningar av informationssäkerheten.

### 11.4 Offentlighetsprincipen

I 316 a och 319 § ingår förslag om sekretess för uppgifter som med stöd av 316 a § lämnas ut till Transport- och kommunikationsverket och dataombudsmannen. Förslaget är av betydelse med avseende på den grundlagsfästa offentlighetsprincipen i 12 § 2 mom. i grundlagen. Sekretessen innebär en begränsning av den principen, eftersom in-formation om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter och konfidentiella radiosändningars innehåll och existens som lämnas ut till myndigheter med stöd av den föreslagna 316 a § är sekretessbelagda, om det inte uttryckligen föreskrivs om undantag från sekretessen i lag.

Kärnan i offentlighetsprincipen är att garantera förutsättningarna för kritik och övervakning av maktutövningen och myndigheternas verksamhet (RP 309/1993 rd, s. 62, och GrUU 43/1998 rd, s. 2–3). De sekretessbelagda uppgifterna gäller situationer där uppgifter om kränkningar av eller hot om kränkningar av informationssäkerheten lämnas ut för att utreda och förebygga sådana kränkningar eller hot om kränkningar. Uppgifterna hör inte till kärnan för offentlighetsprincipen. Om de uppgifter som lämnas ut är offentliga medan en kränkning av informationssäkerheten utreds, kan detta förutses orsaka väsentlig olägenhet för det syfte i vilket uppgifterna lämnas ut till en myndighet. Dessutom måste det göras en intresseavvägning mellan offentlighetsprincipen och skyddet för förtroliga meddelanden enligt 10 § i grundlagen, vilket talar för att de uppgifter som lämnas ut ska vara sekretessbelagda på grund av de skyddsintressen som gäller skyddet för förtroliga meddelanden. Begränsad uppgiftsoffentlighet gör förslaget mer godtagbarhet med avseende på det skydd för förtroliga meddelanden som garanteras i 10 § i grundlagen. Dessutom har det godkänts som utgångspunkt för den gällande lagen om tjänster inom elektronisk kommunikation att Transport- och kommunikationsverket ska sörja för sekretess för sådana uppgifter om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter och konfidentiella radiosändningars innehåll och existens som verket fått med stöd av lagen, om det

inte i lag föreskrivs ett uttryckligt undantag från sekretessen. Med anledning av det som anförs ovan anses det att de ändringar som föreslås i 316 a och 319 § i fråga om begränsning av offentlighetsprincipen är en ändring som är godtagbar med avseende på de allmänna krav som gäller för begränsning av grundläggande fri- och rättigheter.

### 11.5 Sammanfattning

Regeringen anser att det i propositionen inte föreslås några sådana bestämmelser som skulle innebära att lagförslaget inte kan behandlas i vanlig lagstiftningsordning. På grund av de ovan beskrivna aspekterna på skyddet för förtroliga meddelanden anser regeringen det dock önskvärt att ett utlåtande om propositionen inhämtas hos grundlagsutskottet.

*Kläm*

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

**1.**

# Lag

**om ändring av lagen om tjänster inom elektronisk kommunikation**

I enlighet med riksdagens beslut

*upphävs* i lagen om tjänster inom elektronisk kommunikation (917/2014) 250 § 4 mom., sådant det lyder i lag 52/2019,

*ändras* 309 §, 316 § 5 mom. och 319 §, sådana de lyder i lag 1003/2018, samt

*fogas* till lagen nya 316 a och 319 a § som följer:

309 §

*Handräckning*

Transport- och kommunikationsverket har rätt att få handräckning av polisen, Tullen och Gränsbevakningsväsendet för tillsynen över efterlevnaden av och för verkställigheten av denna lag samt bestämmelser som utfärdats och föreskrifter som meddelats med stöd av den. Transport- och kommunikationsverket har rätt att som handräckning av polisen, skyddspolisen och Försvarsmakten få experthjälp, utrustning, lokaler och anordningar för att utreda och undanröja verkningarna av betydande kränkningar av informationssäkerheten eller allvarliga hot om betydande kränkningar av informationssäkerheten. Transport- och kommunikationsverket har rätt att få handräckning av Försvarsmakten för att utreda orsakerna till störningar i radiokommunikationen.

Transport- och kommunikationsverket kan på begäran som handräckning ge andra myndigheter experthjälp, utrustning, lokaler och anordningar.

För kostnaderna för handräckningen svarar den som begärt handräckning, om inte något annat avtalas om saken. En förutsättning för att lämna handräckning är att det inte äventyrar utförandet av andra viktiga uppgifter som enligt lag ska skötas av den myndighet som lämnar handräckning.

Lämnande av handräckning enligt 1 och 2 mom. berättigar inte Transport- och kommunikationsverket att till andra myndigheter lämna ut information om meddelanden, förmedlingsuppgifter eller lokaliseringsuppgifter eller om konfidentiella radiosändningars innehåll och existens.

316 §

*Behandling och utplåning av uppgifter om kommunikation och lokalisering*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Den rätt att få information som avses i denna paragraf gäller inte uppgifter som avses i 15 kap. 14 § i kreditinstitutslagen (610/2014) eller i 17 kap. 20 § 1 mom. i rättegångsbalken, och inte heller sådan kommunikation i samband med skötsel av myndighetsuppgifter som utövas i myndighetsnät eller i en kommunikationstjänst med anknytning till myndighetskommunikation.

316 a §

*Kommunikationsförmedlares rätt att lämna information till Transport- och kommunikationsverket*

Vad som föreskrivs i 136 § 4 mom. hindrar inte en kommunikationsförmedlare från att lämna information till Transport- och kommunikationsverket om sådana förmedlingsuppgifter eller elektroniska meddelanden som förmedlaren behandlar med stöd av 272 §, om det behövs för att utreda eller förebygga kränkningar av eller hot mot informationssäkerheten. Bestämmelser om sådana allmänna behandlingsprinciper för kommunikationsförmedlare som tillämpas på behandling av uppgifter finns i 137 §. På sekretess och utlämnande av uppgifter tillämpas vad som i 319 och 319 a § föreskrivs om sekretess och utlämnande av uppgifter.

319 §

*Tystnadsplikt och utlämnande av information som gäller meddelanden*

Sådana uppgifter som Transport- och kommunikationsverket och dataombudsmannen med stöd av 316, 316 a och 317 § har fått och skaffat om meddelanden, förmedlingsuppgifter och lokaliseringsuppgifter samt om innehållet i och existensen av konfidentiella radiosändningar är sekretessbelagda.

Transport- och kommunikationsverket har trots sekretessen enligt 1 mom. och andra begränsningar som gäller utlämnande av uppgifter rätt att lämna ut förmedlingsuppgifter och andra uppgifter som verket fått i samband med insamling av information om och utredning av kränkningar av informationssäkerheten till

1) en kommunikationsförmedlare, en leverantör av mervärdestjänster, ett företag, en organisation, en abonnent och en användare, om denne har blivit utnyttjad i samband med kränkningen av informationssäkerheten eller har blivit eller sannolikt kan bli utsatt för en sådan kränkning, och om det enligt Transport- och kommunikationsverkets bedömning finns skäl att misstänka att det har begåtts ett sådant brott som nämns i 316 § 2 mom. 1–12 punkten,

2) en sådan i en annan stat verksam myndighet eller annan motsvarande aktör eller sådana institutioner, organ eller byråer inom Europeiska unionen eller Nordatlantiska fördragsorganisationen som har till uppgift att förebygga eller utreda kränkningar av informationssäkerheten som är riktade mot kommunikationsnät och kommunikationstjänster.

Transport- och kommunikationsverket har rätt att lämna ut information enligt vad som föreskrivs i 2 mom. endast i den utsträckning som behövs för att förebygga och utreda kränkningar av informationssäkerheten. Utlämnandet får inte begränsa skyddet av konfidentiella meddelanden och integritetsskyddet mer än vad som är nödvändigt.

Vad som föreskrivs i 1 mom. hindrar inte att förmedlingsuppgifter lämnas ut till en annan myndighet, om det behövs för utredning av eller åtal för brott som gäller orsakande av radiostörningar eller för avhjälpande eller begränsning av störningar av radiokommunikation.

319 a §

*Utlämnande av information vid betydande kränkningar av eller hot mot informationssäkerheten*

Utöver vad som föreskrivs någon annanstans i lag har Transport- och kommunikationsverket, polisen, skyddspolisen och Försvarsmakten trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att till varandra lämna ut sådana förmedlingsuppgifter, sådan information om meddelanden och sådana andra uppgifter som gäller betydande

kränkningar av informationssäkerheten eller allvarliga hot om betydande kränkningar av informationssäkerheten och som är nödvändiga för att utreda, förebygga eller undanröja verkningarna av sådana betydande kränkningar av informationssäkerheten eller allvarliga hot om betydande kränkningar av informationssäkerheten som har eller hotar ha allvarliga skadliga konsekvenser för

1) det allmännas beslutsförmåga eller myndigheternas verksamhetsförutsättningar,
2) den nationella säkerheten eller försvaret,
3) nödvändiga tjänster inom social- och hälsovården eller räddningsväsendet,
4) energi-, vatten-, livsmedels- eller läkemedelsförsörjningen eller andra nödvändiga nyttigheter,
5) nödvändiga betalnings- och värdepapperstjänster,
6) samhällets kritiska trafik- och kommunikationstjänster,
7) informations- och kommunikationstekniska tjänster eller informationsmaterial som upprätthåller de funktioner som avses i 1–6 punkten.

Uppgifter som lämnats ut med stöd av 1 mom. får användas endast för att utreda, förebygga eller undanröja verkningarna av kränkningar av informationssäkerheten eller allvarliga hot om kränkningar av informationssäkerheten. Uppgifterna får inte användas för något annat ändamål. Onödiga uppgifter ska raderas. På utplåning av uppgifter tillämpas vad som i 316 § 4 mom. föreskrivs om utplåning av uppgifter.

Vid behandlingen av uppgifter som lämnats ut med stöd av 1 mom. ska i fråga om begränsningar i användningen av uppgifter, vidarelämnande av uppgifter och återsändande av utlämnat material iakttas vad som anges i de villkor som den som lämnat ut uppgifterna ställt. Den utlämnande myndigheten ska i samband med utlämnandet meddela om uppgifterna som lämnas ut är förenade med sådana begränsningar.

---

Denna lag träder i kraft den 20 .

---

**2.**

# Lag

**om ändring av29 § i lagen om behandling av personuppgifter inom Försvarsmakten**

I enlighet med riksdagens beslut

*ändras* i lagen om behandling av personuppgifter inom Försvarsmakten (332/2019) 29 § 1 mom. 18 punkten som följer:

29 §

*Rätt att lämna ut personuppgifter för fullgörande av lagstadgade uppgifter*

Trots sekretessbestämmelserna får Försvarsmakten genom en teknisk anslutning eller som en datamängd till en annan myndighet och till en sammanslutning som tillsatts för att sköta ett offentligt uppdrag lämna ut personuppgifter som behövs för fullgörande av dess lagstadgade uppgifter, enligt följande:

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

18) till Transport- och kommunikationsverket för skötseln av uppgifter enligt 3 § i lagen om Transport- och kommunikationsverket (935/2018) och 304 § 1, 7, 9 och 10 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014),

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

_____

Denna lag träder i kraft den 20 .

_____

**3.**

# Lag

**om ändring av 22 § i lagen om behandling av personuppgifter i polisens verksamhet**

I enlighet med riksdagens beslut

*ändras* i lagen om behandling av personuppgifter i polisens verksamhet (616/2019) 22 § 1 mom. 1 punkten som följer:

22 §

*Övrigt utlämnande av personuppgifter till myndigheter*

Polisen får trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd lämna ut sådana personuppgifter som avses i 5–8, 11 och 12 § för en uppgift som myndigheten har enligt lag, enligt följande:

1) till Transport- och kommunikationsverket de uppgifter i enlighet med 197 och 217 § i lagen om transportservice som är nödvändiga för skötseln av verkets lagstadgade uppgifter och till Transport- och kommunikationsverket för skötseln av verkets uppgifter enligt 3 § i lagen om Transport- och kommunikationsverket (935/2018) och 304 § 1, 7, 9 och 10 punkten i lagen om tjänster inom elektronisk kommunikation,

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———————

Helsingfors den 27 oktober 2022

**Statsminister**

**Sanna Marin**

Kommunikationsminister Timo Harakka

*Bilaga*
*Parallelltext*

**1.**

# Lag

**om ändring av lagen om tjänster inom elektronisk kommunikation**

I enlighet med riksdagens beslut

*upphävs* i lagen om tjänster inom elektronisk kommunikation (917/2014) 250 § 4 mom., sådant det lyder i lag 52/2019,

*ändras* 309 §, 316 § 5 mom. och 319 §, sådana de lyder i lag 1003/2018, samt

*fogas* till lagen nya 316 a och 319 a § som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 250 § | 250 § |
| *Myndighetsabonnemang* | *Myndighetsabonnemang* |
| — — — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — — — |
| På sådan kommunikation som utövas i samband med skötsel av myndighetsuppgifter i myndighetsnät eller i kommunikationstjänsten med anknytning till myndighetskommunikation tillämpas inte 316 §. | (upphävs) |
| 309 § | 309 § |
| *Handräckning* | *Handräckning* |
| Transport- och kommunikationsverket har rätt att få handräckning av polisen, Tullen och Gränsbevakningsväsendet för tillsynen över efterlevnaden av och för verkställigheten av denna lag samt bestämmelser som utfärdats och föreskrifter som meddelats med stöd av den. Transport- och kommunikationsverket har rätt att få handräckning av försvarsmakten för att utreda orsakerna till störningar i radiokommunikationen. | Transport- och kommunikationsverket har rätt att få handräckning av polisen, Tullen och Gränsbevakningsväsendet för tillsynen över efterlevnaden av och för verkställigheten av denna lag samt bestämmelser som utfärdats och föreskrifter som meddelats med stöd av den. Transport- och kommunikationsverket har rätt *att som handräckning av polisen, skyddspolisen och Försvarsmakten få experthjälp, utrustning, lokaler och anordningar för att utreda och undanröja verkningarna av betydande kränkningar av informationssäkerheten eller allvarliga hot om betydande kränkningar av informationssäkerheten.* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| Transport- och kommunikationsverket kan på begäran ge andra myndigheter experthjälp som handräckning. *Beslut om att lämna handräckning fattas av kommunikationsministeriet.* För kostnaderna för den handräckning som *Transport- och kommunikationsverket lämnar* svarar den som begärt handräckning, om inte något annat avtalas om saken. | Transport- och kommunikationsverket har rätt att få handräckning av Försvarsmakten för att utreda orsakerna till störningar i radiokommunikationen.<br>Transport- och kommunikationsverket kan på begäran som *handräckning ge andra myndigheter experthjälp, utrustning, lokaler och anordningar.*<br>För kostnaderna för handräckningen svarar den som begärt handräckning, om inte något annat avtalas om saken. E*n förutsättning för att lämna handräckning är att det inte äventyrar utförandet av andra viktiga uppgifter som enligt lag ska skötas av den myndighet som lämnar handräckning.* |
| Lämnande av handräckning enligt 2 mom. berättigar inte Transport- och kommunikationsverket att till andra myndigheter lämna ut information om meddelanden, förmedlingsuppgifter eller lokaliseringsuppgifter eller om konfidentiella radiosändningars innehåll och existens. | Lämnande av handräckning enligt 1 *och 2* mom. berättigar inte Transport- och kommunikationsverket att till andra myndigheter lämna ut information om meddelanden, förmedlingsuppgifter eller lokaliseringsuppgifter eller om konfidentiella radiosändningars innehåll och existens. |
| 316 § | 316 § |
| *Behandling och utplåning av uppgifter om kommunikation och lokalisering* | *Behandling och utplåning av uppgifter om kommunikation och lokalisering* |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| Den rätt att få information som avses i denna paragraf gäller inte uppgifter som avses i 15 kap. 14 § i kreditinstitutslagen (610/2014) eller i 17 kap. 20 § 1 mom. i rättegångsbalken. | Den rätt att få information som avses i denna paragraf gäller inte uppgifter som avses i 15 kap. 14 § i kreditinstitutslagen (610/2014) eller i 17 kap. 20 § 1 mom. i rättegångsbalken, *och inte heller sådan kommunikation i samband med skötsel av myndighetsuppgifter som utövas i myndighetsnät eller i en kommunikationstjänst med anknytning till myndighetskommunikation.* |
| | 316 a § |
| | *Kommunikationsförmedlares rätt att lämna information till Transport- och kommunikationsverket* |
| (Ny) | *Vad som föreskrivs i 136 § 4 mom. hindrar inte en kommunikationsförmedlare från att lämna information till Transport- och kommu-* |

*Gällande lydelse*

*Föreslagen lydelse*

*nikationsverket om sådana förmedlingsuppgifter eller elektroniska meddelanden som förmedlaren behandlar med stöd av 272 §, om det behövs för att utreda eller förebygga kränkningar av eller hot mot informationssäkerheten. Bestämmelser om sådana allmänna behandlingsprinciper för kommunikationsförmedlare som tillämpas på behandling av uppgifter finns i 137 §. På sekretess och utlämnande av uppgifter tillämpas vad som i 319 och 319 a § föreskrivs om sekretess och utlämnande av uppgifter.*

319 §

*Tystnadsplikt och utlämnande av information som gäller meddelanden*

Sådana uppgifter som Transport- och kommunikationsverket och dataombudsmannen med stöd av 316 och 317 § har fått och skaffat om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter samt om innehållet i och existensen av konfidentiella radiosändningar är sekretessbelagda.

Transport- och kommunikationsverket har trots sekretessen enligt 1 mom. och andra begränsningar som gäller utlämnande av uppgifter rätt att lämna ut förmedlingsuppgifter och andra uppgifter som verket fått i samband med insamling av information om och utredning av kränkningar av informationssäkerheten till

1) en kommunikationsförmedlare, en leverantör av mervärdestjänster, ett företag, en organisation, en abonnent och en användare, om denna har blivit utnyttjad i samband med kränkningen av informationssäkerheten eller har blivit eller sannolikt kan bli utsatt för en sådan kränkning, och om det enligt Transport- och kommunikationsverkets bedömning finns skäl att misstänka att det har begåtts ett sådant brott som nämns i 316 § 2 mom. 1–12 punkten,

2) en sådan i en annan stat verksam myndighet eller annan motsvarande aktör som har till uppgift att förebygga eller utreda sådana kränkningar av informationssäkerheten som är riktade mot kommunikationsnät och kommunikationstjänster.

319 §

*Tystnadsplikt och utlämnande av information som gäller meddelanden*

Sådana uppgifter som Transport- och kommunikationsverket och dataombudsmannen med stöd av 316, *316 a* och 317 § har fått och skaffat om meddelanden, förmedlingsuppgifter och lokaliseringsuppgifter samt om innehållet i och existensen av konfidentiella radiosändningar är sekretessbelagda.

Transport- och kommunikationsverket har trots sekretessen enligt 1 mom. och andra begränsningar som gäller utlämnande av uppgifter rätt att lämna ut förmedlingsuppgifter och andra uppgifter som verket fått i samband med insamling av information om och utredning av kränkningar av informationssäkerheten till

1) en kommunikationsförmedlare, en leverantör av mervärdestjänster, ett företag, en organisation, en abonnent och en användare, om denne har blivit utnyttjad i samband med kränkningen av informationssäkerheten eller har blivit eller sannolikt kan bli utsatt för en sådan kränkning, och om det enligt Transport- och kommunikationsverkets bedömning finns skäl att misstänka att det har begåtts ett sådant brott som nämns i 316 § 2 mom. 1–12 punkten,

2) en sådan i en annan stat verksam myndighet eller annan motsvarande aktör eller sådana institutioner, *organ eller byråer inom Europeiska unionen eller Nordatlantiska fördragsorganisationen* som har till uppgift att förebygga

*Gällande lydelse*

Transport- och kommunikationsverket har rätt att lämna ut information enligt vad som föreskrivs i 2 mom. endast i den utsträckning som behövs för att förebygga och utreda kränkningar av informationssäkerheten. Utlämnandet får inte begränsa skyddet av konfidentiella meddelanden och integritetsskyddet mer än vad som är nödvändigt.

Vad som föreskrivs i 1 mom. hindrar inte att förmedlingsuppgifter lämnas ut till en annan myndighet, om det behövs för utredning av eller åtal för brott som gäller orsakande av radiostörningar eller för avhjälpande eller begränsning av störningar av radiokommunikation.

*När Transport- och kommunikationsverket bestämmer vilka myndigheter och andra aktörer som avses i 2 mom. 2 punkten ska det samarbeta med kommunikationsministeriet. Om ett beslut som gäller till vem information får lämnas ut kan ha en avsevärd samhällelig betydelse eller konsekvenser för den allmänna utvecklingen av tjänster för elektronisk kommunikation, ska kommunikationsministeriet bestämma till vilka myndigheter och andra aktörer Transport- och kommunikationsverket får lämna ut information som avses i 2 mom.*

*Föreslagen lydelse*

eller utreda kränkningar av informationssäkerheten som är riktade mot kommunikationsnät och kommunikationstjänster.

Transport- och kommunikationsverket har rätt att lämna ut information enligt vad som föreskrivs i 2 mom. endast i den utsträckning som behövs för att förebygga och utreda kränkningar av informationssäkerheten. Utlämnandet får inte begränsa skyddet av konfidentiella meddelanden och integritetsskyddet mer än vad som är nödvändigt.

Vad som föreskrivs i 1 mom. hindrar inte att förmedlingsuppgifter lämnas ut till en annan myndighet, om det behövs för utredning av eller åtal för brott som gäller orsakande av radiostörningar eller för avhjälpande eller begränsning av störningar av radiokommunikation.

(upphävs)

(ny)

319 a §

*Utlämnande av information vid betydande kränkningar av eller hot mot informationssäkerheten*

*Utöver vad som föreskrivs någon annanstans i lag har Transport- och kommunikationsverket, polisen, skyddspolisen och Försvarsmakten trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att till varandra lämna ut sådana förmedlingsuppgifter, sådan information om meddelanden och sådana andra uppgifter som gäller betydande kränkningar av informationssäkerheten eller allvarliga hot*

*Gällande lydelse*

*Föreslagen lydelse*

*om betydande kränkningar av informationssäkerheten och som är nödvändiga för att utreda, förebygga eller undanröja verkningarna av sådana betydande kränkningar av informationssäkerheten eller allvarliga hot om betydande kränkningar av informationssäkerheten som har eller hotar ha allvarliga skadliga konsekvenser för*

*1) det allmännas beslutsförmåga eller myndigheternas verksamhetsförutsättningar,*

*2) den nationella säkerheten eller försvaret,*

*3) nödvändiga tjänster inom social- och hälsovården eller räddningsväsendet,*

*4) energi-, vatten-, livsmedels- eller läkemedelsförsörjningen eller andra nödvändiga nyttigheter,*

*5) nödvändiga betalnings- och värdepapperstjänster,*

*6) samhällets kritiska trafik- och kommunikationstjänster,*

*7) informations- och kommunikations-tekniska tjänster eller informations-material som upprätthåller de funktioner som avses i 1–6 punkten.*

*Uppgifter som lämnats ut med stöd av 1 mom. får användas endast för att utreda, förebygga eller undanröja verkningarna av kränkningar av informationssäkerheten eller allvarliga hot om kränkningar av informationssäkerheten. Uppgifterna får inte användas för något annat ändamål. Onödiga uppgifter ska raderas. På utplåning av uppgifter tillämpas vad som i 316 § 4 mom. föreskrivs om utplåning av uppgifter.*

*Vid behandlingen av uppgifter som lämnats ut med stöd av 1 mom. ska i fråga om begränsningar i användningen av uppgifter, vidarelämnande av uppgifter och återsändande av utlämnat material iakttas vad som anges i de villkor som den som lämnat ut uppgifterna ställt. Den utlämnande myndigheten ska i samband med utlämnandet meddela om uppgifterna som lämnas ut är förenade med sådana begränsningar.*

---

Denna lag träder i kraft den 20 .

---

**2.**

# Lag

**om ändring av av 29 § i lagen om behandling av personuppgifter inom Försvarsmakten**

I enlighet med riksdagens beslut
*ändras* i lagen om behandling av personuppgifter inom Försvarsmakten (332/2019) 29 § 1 mom. 18 punkten som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 29 § | 29 § |
| *Rätt att lämna ut personuppgifter för fullgörande av lagstadgade uppgifter* | *Rätt att lämna ut personuppgifter för fullgörande av lagstadgade uppgifter* |
| Trots sekretessbestämmelserna får Försvarsmakten genom en teknisk anslutning eller som en datamängd till en annan myndighet och till en sammanslutning som tillsatts för att sköta ett offentligt uppdrag lämna ut personuppgifter som behövs för fullgörande av dess lagstadgade uppgifter, enligt följande: | Trots sekretessbestämmelserna får Försvarsmakten genom en teknisk anslutning eller som en datamängd till en annan myndighet och till en sammanslutning som tillsatts för att sköta ett offentligt uppdrag lämna ut personuppgifter som behövs för fullgörande av dess lagstadgade uppgifter, enligt följande: |
| — — — — — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — — — — — |
| 18) till Cybersäkerhetscentret vid Transport- och kommunikationsverket för skötseln av uppgifter enligt 3 § i lagen om Transport- och kommunikationsverket (935/2018), | 18) till Transport- och kommunikationsverket för skötseln av uppgifter enligt 3 § i lagen om Transport- och kommunikationsverket (935/2018) *och 304 § 1, 7, 9 och 10 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014),* |
| — — — — — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — — — — — |

Denna lag träder i kraft den 20 .

**3.**

# Lag

**om ändring av 22 § i lagen om behandling av personuppgifter i polisens verksamhet**

I enlighet med riksdagens beslut
*ändras* i lagen om behandling av personuppgifter i polisens verksamhet (616/2019) 22 § 1 mom. 1 punkten som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 22 § | 22 § |
| *Övrigt utlämnande av personuppgifter till myndigheter* | *Övrigt utlämnande av personuppgifter till myndigheter* |
| Polisen får trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd lämna ut sådana personuppgifter som avses i 5–8, 11 och 12 § för en uppgift som myndigheten har enligt lag, enligt följande: | Polisen får trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd lämna ut sådana personuppgifter som avses i 5–8, 11 och 12 § för en uppgift som myndigheten har enligt lag, enligt följande: |
| 1) till Transport- och kommunikationsverket de uppgifter i enlighet med 197 och 217 § i lagen om transportservice som är nödvändiga för skötseln av verkets lagstadgade uppgifter, | 1) till Transport- och kommunikationsverket de uppgifter i enlighet med 197 och 217 § i lagen om transportservice som är nödvändiga för skötseln av verkets lagstadgade uppgifter *och till Transport- och kommunikationsverket för skötseln av verkets uppgifter enligt 3 § i lagen om Transport- och kommunikationsverket (935/2018) och 304 § 1, 7, 9 och 10 punkten i lagen om tjänster inom elektronisk kommunikation,* |
| — — — — — — — — — — — — — — | — — — — — — — — — — — — — — |

Denna lag träder i kraft den 20 .