

U 13/2013 vp

Valtioneuvoston kirjelmä Eduskunnalle Euroopan parlamentin ja neuvoston direktiiviksi verkko- ja tietoturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella

Perustuslain 96 §:n 2 momentin mukaisesti lähetetään eduskunnalle Euroopan komission 7 päivänä helmikuuta 2013 antama ehdotus Euroopan parlamentin ja neuvoston direktiiviksi verkko- ja tietoturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella (COM(2013) 48 lopullinen) sekä ehdotuksesta laadittu muistio.

viksi verkko- ja tietoturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella (COM(2013) 48 lopullinen) sekä ehdotuksesta laadittu muistio.

Helsingissä 20 päivänä maaliskuuta 2013

Liikenneministeri *Merja Kyllönen*

Neuvotteleva virkamies Timo Kievari

LIIKENNE- JA VIESTINTÄMINISTERIÖN

MUISTIO

EU/2013/0630

EUROOPAN KOMISSION EHDOTUS EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI VERKKO- JA TIETOTURVALLISUUDEN KORKEAN TASON VARMISTAMISEKSI EUROOPAN UNIONIN ALUEELLA (COM(2013) 48 LOPULLINEN)**1 Yleistä**

Euroopan komissio antoi 7 päivänä helmikuuta 2013 ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi verkko- ja tietoturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella (jäljempänä tietoturvadirektiivi).

Direktiiviehdotuksella jäsenvaltiot velvoitettaisiin ensinnäkin laatimaan verkko- ja tietoturvastrategia sekä nimeämään kansallinen toimivaltainen viranomainen, jolla on riittävät taloudelliset ja henkilöstöresurssit turvariskien ja -poikkeamien ennaltaehkäisyä ja käsittelyä sekä niihin reagoimista varten.

Toiseksi direktiivillä luotaisiin jäsenvaltioiden ja komission välinen yhteistyömekanismi, jonka keinoin voitaisiin vaihtaa ennakkovaroituksia tietoturvariskeistä ja -poikkeamista, tehdä yhteistyötä niiden ratkaisemisessa ja järjestää säännöllisiä vertaisarviointeja sekä harjoituksia.

Kolmanneksi direktiivi velvoittaisi eräiden yhteiskunnan keskeisten alojen (rahoituspalvelut, liikenne, energia, terveys) kriittisten infrastruktuurien ylläpitäjät sekä keskeisimmät tietoyhteiskunnan palvelun tarjoajat ja julkishallinnot ottamaan käyttöön riskinhallintakäytänteitä ja raporttoimaan ylläpitämissä keskeisiin palveluihin kohdistuvista merkittävistä tietoturva-poikkeamista.

EU:n kyberturvallisuusstrategia

Euroopan komissio antoi 7 päivänä helmikuuta 2013 tiedonannon Euroopan unionin kyberturvallisuusstrategiaksi. Strategian yhtenä tavoitteena on kehittää tietoyhteiskunnan vankkarakenteisuutta parantamalla vaurautuneisuutta, yhteistyötä, osaamista ja tiedonvaihtoa verkko- ja tietoturvan saralla. Direktiiviehdotuksella toimeenpannaan strategian linjauksia.

Ehdotuksen tavoitteet

Direktiiviehdotuksen tavoitteina on muun muassa turvata verkko- ja tietoturvallisuuden korkean taso Euroopan Unionissa ja sen jäsenmaissa (1 artikla). Direktiivi olisi vähimmäisdirektiivi, eikä se estäisi korkeamman turvatason säätämistä kansallisesti (2 artikla). Direktiivi tulisi saattaa kansallisesti voimaan 18 kuukauden kuluessa sen hyväksymisestä (21 artikla).

2 Ehdotuksen pääasiallinen sisältö*Kansallinen kehys verkko- ja tietoturvallisuudelle*

Direktiiviehdotuksen mukaan jäsenvaltioiden olisi laadittava kansallinen verkko- ja tietoturvallisuusstrategia sekä sen osana yhteistyösuunnitelma (5 artikla).

Jäsenvaltioiden tulisi osoittaa kansallinen verkko- ja tietojärjestelmien turvallisuusvi-

ranomainen (jäljempänä tietoturvaviranomainen), jonka tehtävänä olisi muun muassa valvoa direktiivin säännösten ja direktiivin nojalla säädettävien tietoturvallisuuden vähimmäisvaatimusten toteutumista; vastaanottaa ja lähettää direktiivin mukaisia ilmoituksia ja varoituksia tietoturvaloukkauksista; osallistua yhteistyöhön kansallisten esitutkinta- ja tietosuojaviranomaisten kanssa sekä jakaa tietoa ja toimia yhteistyössä kansainvälisten vastinpariensä kanssa (6 artikla). Lisäksi kuhunkin jäsenvaltioon tulisi perustaa tietoturvapoikkeamien ja -riskien selvittämiseen erikoitunut ryhmä, joista käytetään kansainvälisesti nimitystä ”Computer Emergency Response Team” (jäljempänä CERT), ja joka voisi direktiivin mukaan toimia osana tietoturvaviranomaista (7 artikla).

Yhteistyö eri viranomaisten kesken

Eri jäsenmaiden tietoturvaviranomaiset ja komissio muodostaisivat direktiivin mukaan yhteistyöverkoston, jossa toimivien tietoturvaviranomaisten tehtävinä olisi muun muassa jakaa tietoturvapoikkeamien ja riskien varoitustietoja; varmistaa poikkeamiin reagoiminen yhteensopivalla tavalla; julkaista tietoja kulloisistakin varoituksista ja niihin reagoimisesta; arvioida pyydettyä kansallisia strategioita, yhteistyösuunnitelmia ja CERT-ryhmien toimintaa; toimeenpanna verkko- ja tietoturvallisuuden harjoituksia unionissa sekä toimia yhteistyössä ja vaihtaa tietoa Europoliin sijoitetun Euroopan tietoverkkorikosturvaston ja muiden keskeisten eurooppalaisten toimielimien kanssa etenkin, jos ne toimivat tietosuojan, energianjakelun, liikenteen, pankkitoiminnan, pörssikaupan tai terveydenhuollon aloilla. (8 artikla)

Verkoston välillä luottamuksellista tietoa vaihdettaisiin ainoastaan tietoturvallisilla järjestelmillä ja turvallisilla tiedonvaihtokanavilla. Direktiiviehdotuksessa komissiolle delegoitaisiin norminantovalta niistä vaatimuksista, jotka olisivat tietoturvallisen järjestelmän ja tiedonvaihtokanavien käytön edellytyksenä (9 artikla).

Tietoturvaviranomaisen tulisi varoittaa ennakolta muissa jäsenvaltioissa sijaitsevia vastinparejaan ja komissiota tietoturvallisuutta vaarantavista turvariskeistä ja poikkeamista.

Tässä tarkoituksessa tietoturvaviranomaisilla ja komissiolla olisi velvollisuus jakaa hallussaan olevaa tarpeellista tietoa turvariskin tai -poikkeaman arvioimiseksi. Komissio voisi myös vaatia jäsenvaltioita toimittamaan lisätietoja. Mikäli ennakkovaroitukseen liittyisi rikosepäily, tulisi kansallisen viranomaisen tai komission ilmoittaa tästä Europolin yhteydessä toimivalle Euroopan tietoverkkorikoskeskukselle. Komissiolla olisi myös toimivalta määritellä kynnys, jonka ylittävistä tapahtumista tai riskeistä ennakkovaroitus tulisi tehdä (10 artikla).

Ennakkovaroituksen jälkeen yhteistyöverkoston viranomaisten tulisi sopia siitä, miten ne voivat unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti reagoida käsilä olevan tapaukseen koordinoitulla tavalla. Tiedot kansallisista toimenpiteistä tulisi jakaa muille verkoston viranomaisille (11 artikla).

Komissiolle delegoitaisiin toimivalta hyväksyä unionille yhteisen verkko- ja tietoturvallisuuden yhteistyösuunnitelma. Suunnitelmassa määriteltäisiin ennakkovaroituksia koskevien tietojen keräämisen, jakamisen ja arvioinnin muodot sekä menettelytavat. Suunnitelmassa määriteltäisiin niin ikään ne menettelytavat, joiden mukaisesti tapauksiin reagoiminen tulisi sovittaa yhteen yhteistyöverkoston viranomaisissa. Suunnitelmassa olisi lueteltu myös toimenpiteet verkko- ja tietoturvallisuutta koskevien harjoitusten ja osaamisen kehittämiseksi (12 artikla).

Ehdotuksen mukaan komissio voisi solmia sellaisia sopimuksia unionin ulkopuolisten kolmansien maiden ja järjestöjen kanssa, jotka mahdollistaisivat niiden osallistumisen verkottuneiden kansallisten viranomaisten toimintaan (13 artikla).

Verkkojen ja tietojärjestelmien turvallisuusvaatimukset sekä poikkeamien ilmoitusvelvollisuus

Direktiivin mukaan jäsenvaltioiden tulee varmistaa, että Unionin alueella toimivat julkishallinnot ja eräät yritykset toteuttavat tarkoituksenmukaiset toimenpiteet verkko- ja tietojärjestelmiensä turvallisuuteen kohdistuvien riskien hallitsemiseksi, jotta niiden toiminta voisi jatkua mahdollisimman häiriöt-

tömästi turvapoikkeamista huolimatta. Turvallisuusvaatimukset koskisivat julkishallinnon lisäksi rahoituspalvelujen, liikenteen, energia-alan ja terveydenhuollon toimivuuden kannalta kriittisten infrastruktuurien ylläpitäjiä. Lisäksi vaatimukset koskisivat eräitä keskeisiä tietoyhteiskunnan palvelujen toiminnan mahdollistavia palveluntarjoajia. Tarkempi soveltamisala on kuvattu direktiiviehdotuksen liitteessä II (14 artikla).

Soveltamisalaan kuuluvien tahojen tulisi myös ilmoittaa tietoturaviranomaiselle sellaisista turvapoikkeamista, jotka vaarantavat merkittävällä tavalla niiden toiminnan turvallisuuden. Direktiiviehdotuksessa delegoitaisiin komissiolle toimivaltaa määritellä niitä ilmoituskynnyksiä, joiden ylittyessä ilmoitusvelvollisuus olisi käsillä. Niin ikään komissiolle olisi delegoitu toimivaltaa säätää niistä menettelytavoista, joita ilmoituksissa tulisi noudattaa. Direktiiviehdotuksen mukaan tietoturaviranomainen voisi yleisen edun vaatiessa tiedottaa tai velvoittaa ilmoituksen tekijän itse tiedottamaan julkisesti niistä tietoturvallisuuden poikkeamista, jotka ovat ilmoitusvelvollisuuden alaisia (14 artikla).

Tietoturaviranomaisella olisi valtuudet tutkia tapaukset, joissa julkishallinnot tai yritykset eivät ole noudattaneet velvoitteitaan. Tietoturaviranomaisella olisi valtuudet vaatia julkishallinnoilta ja yrityksiltä tarvittavia tietoja niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi sekä velvoittaa ne suorittamaan ulkopuolisen tekemä turvallisuusarviointi. Viranomaisilla tulisi olla valtuus antaa sitovia ohjeita (15 artikla).

Tietoturaviranomaisen tulisi toimia läheisessä yhteistyössä henkilötietojen tietosuojasta vastaavien tietosuojaviranomaisten kanssa silloin kun käsillä on tapaus, joka vaarantaa henkilötietojen suojan. Tietoturaviranomaisen tulisi ilmoittaa esitutkintaviranomaisille sellaisista turvapoikkeamista, joihin liittyy epäily vakavista rikoksista (15 artikla).

Direktiiviehdotuksen mukaan jäsenvaltioiden tulisi kansallisesti kannustaa sellaisten standardien omaksumiseen, jotka olisivat olennaisia verkko- ja tietoturvallisuuden kannalta. Komissio pitäisi ja julkaisisi listaa tällaisia standardeista (16 artikla).

Jäsenmaiden tulisi varmistaa, että direktiivin vastaisesta toiminnasta rangaistaisiin tehokkailla, oikeasuhteisilla ja ennaltaehkäisevillä seuraamuksilla (17 artikla).

3 Ehdotuksen vaikutukset

Vaikutukset lainsäädäntöön

Direktiivin soveltamisalan ulkopuolelle jäävien teleyritysten osalta tietoturvallisuuden vähimmäisvaatimuksista ja ilmoitusmenettelyistä on säädetty sähköisen viestinnän tietosuojalaissa. Laissa on myös tietoturaviranomaisena toimivan Viestintäviraston tietoturvaloukkausten havaintotietojen keräämiseen ja jakamiseen sekä tietoturvaloukkausten selvittämiseen liittyviä tehtäviä koskevat säännökset. Laissa on myös säännökset direktiiviehdotusta vastaavia säännöksiä vähimmäisvaatimuksista ja ilmoitusvelvollisuuksista, jotka koskevat kuitenkin vain teleyrityksiä. Finanssivalvonta on rahoitustarkastuksesta annetun lain (587/2003) nojalla antanut määräyksiä, joissa on osoitettu finanssialan toimijoiden riskienhallintavaatimuksista sekä alan toimijoiden turvapoikkeamien raportointivelvoitteista Finanssivallvonnalle.

Direktiivi edellyttäisi ehdotetussa muodossaan kansallisen lainsäädännön muuttamista muun muassa turvallisuusvaatimusten ja turvapoikkeamista ilmoittamista koskevien velvoitteiden sekä turvallisuusvaatimuksia koskevien arviointivelvoitteiden ja edellä mainittujen velvoitteiden täytäntöönpanon valvonnan osalta.

Liikenne- ja viestintäministeriössä on käynnissä hallitusohjelman mukainen lainsäädäntöhanke, jonka yhteydessä kaikki sähköistä viestintää ja tietoyhteiskunnan palvelujen kysyntää, tarjontaa ja käyttöä koskevat säännökset koottaisiin yhteen lakiin tietoyhteiskuntakaareksi. Direktiivin edellyttämät lainsäädäntötoimenpiteet voitaisiin toteuttaa kootusti osana tietoyhteiskuntakaaren säätämistä tai muuttamalla tietoyhteiskuntakaarta sen tultua voimaan. Säännökset on myös mahdollista toteuttaa osittain osana tietoyhteiskuntakaarta ja osittain osana direktiivin

soveltamisalan piiriin tulevien toimialojen toimintaa ohjaavassa lainsäädännössä.

Suomessa on laadittu ensimmäinen kansallinen tietoturvastrategia jo vuonna 2003. Strategia uusittiin vuonna 2008 ja tammi-kuussa 2013 valtioneuvosto antoi periaatepäätöksen ensimmäiseksi kansalliseksi kyberturvallisuusstrategiaksi.

Vaikutukset viranomaisten toimintaan

Suomessa lukuisia kansallisen tietoturvaviranomaisen tehtäviä on säädetty Viestintäviraston vastuulle. Viestintävirastoon on jo vuonna 2002 perustettu direktiivin edellyttämä kansallinen CERT-ryhmä. Viestintäviraston lakisääteisenä tehtävänä on muun muassa kerätä ja jakaa tietoja tietoturvaloukkauksista sekä niiden uhkista ja selvittää niitä. Viestintävirasto saa tietoja sähköisen viestinnän alalta lakisääteisiin ilmoitusvelvollisuuksiin perustuen teleyrityksiltä sekä toisaalta vapaaehtoisuuteen perustuen Suomen huoltovarmuuden kannalta kriittisiltä yrityksiltä. Lisäksi Viestintäviraston tehtävänä on viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointi sekä tietoturvallisuuden arviointilaitoksien hyväksyminen.

Viestintävirasto neuvottelee parhaillaan valtionhallinnon tietoturvallisuuden yleisestä ohjauksesta vastaavan valtiovarainministeriön kanssa viestintäviraston tietoturvapointeja koskevien palveluiden ulottamisesta myös julkishallintoon siten, että julkishallinnon virastot voisivat hyötyä niistä.

Lisäksi viestintävirasto valvoo sähköisen viestinnän toimintaa ohjaavaa lainsäädäntöä ja muun muassa toimialan yritysten toimintavarmuuteen, jatkuvuuden hallintaan ja häiriötilanteisiin varautumiseen liittyviä säännöksiä. Viestintävirastolle on laissa delegoitu tarkempaa teknistä norminantovaltaa muun muassa sähköisen viestinnän tietoturvallisuuteen liittyvien velvoitteiden toteuttamiseksi.

Finanssivalvonta valvoo muun muassa pankkien ja maksulaitosten tietoturvallisuutta ja tekee niihin tarkastuksia, antaa aihealueeseen liittyvää sääntelyä sekä kerää tietoa järjestelmiin ja tietoturvallisuuteen liittyvistä häiriöistä sekä analysoi niitä.

Valtioneuvoston periaatepäätöksessä kansallisesta kyberturvallisuusstrategiasta tode-

taan, että Viestintäviraston osaksi tulisi perustaa kansallinen kyberturvallisuuskeskus, jonka tehtävät olisivat monin osin linjassa direktiiviehdotuksessa esitettyjen tietoturvaviranomaisen tehtävien kanssa. Viestintävirasto olisikin luontevin viranomainen, jolle ainakin osa direktiivin mukaisista viranomaistehtävistä voitaisiin Suomessa osoittaa.

Taloudelliset vaikutukset

Direktiivi voisi aiheuttaa sellaisille soveltamisalaan kuuluville yrityksille ja julkishallinnon viranomaisille taloudellisia vaikutuksia, jotka eivät toteuttaisi direktiivin mukaisesti tarkoituksenmukaisia teknisiä ja organisatorisia toimenpiteitä verkko- ja tietojärjestelmiensä turvallisuuteen liittyvien riskien hallitsemiseksi. On mahdollista, että myös turvapointeista ilmoittaminen voisi aiheuttaa taloudellisia kustannuksia. Taloudelliset vaikutukset riippuvat kuitenkin ensinnäkin direktiivin kansallisessa voimaannpanossa ratkaistavien turvallisuusvaatimusten laadusta. Toisaalta taloudelliset vaatimukset riippuvat komissiolle ilmoituskynnyksen määrittämiseksi delegoitavan toimivallan käytön laajuudesta ja laadusta.

Tällä hetkellä nettobudjetoidun Viestintäviraston tietoturvaviranomaistehtäviä hoitavan CERT-ryhmän rahoituksesta noin neljännes kerätään teleyrityksiltä perittävänä hallinnollisena tietoturvamaksuna ja kolme neljännestä Huoltovarmuuskeskuksen kanssa solmitun ostopalvelusopimuksen mukaisina vastikkeina niistä tietoturvasuoritteista, joita Viestintävirasto huoltovarmuuskriittisille yrityksille tarjoaa. Julkishallinto ei rahoita Viestintäviraston tietoturvatoimintaa.

Direktiiviehdotuksen myötä ainakin osa Suomessa jo vakiintuneista vapaaehtoisuuteen perustuvista tietoturvailmoitusten käytännöistä muuttuisi direktiivin soveltamisalaan kuuluvia kriittisten infrastruktuurien ylläpitäjiä velvoittaviksi. Samalla CERT-FI:n rahoitusmallia jouduttaisiin mahdollisesti arvioimaan uudelleen. Tarkempia vaikutuksia viranomaisten taloudellisiin tarpeisiin ja henkilöresurssitarpeisiin voidaan arvioida vasta kun tehdään kansallisia ratkaisuja tehtävien osoittamisesta ja niiden laajuudesta.

Tietoyhteiskuntavaikutukset

Direktiiviehdotus lisäisi läpinäkyvyyttä yhteiskunnassa tietoturvapoikkeamista, niihin liittyvistä riskeistä sekä näiden vaikutuksista yhteiskunnan eri toiminnoille. Direktiivi edistäisi tiedonvaihtoa ja viranomaisyhteistyötä jäsenvaltioiden välillä rajat ylittävissä tietoturvaloukkauksissa. Direktiivin täytäntöönpano olisi omiaan lisäämään luottamusta sähköisiin tieto- ja viestintäjärjestelmiin sekä niistä riippuvaisiin yhteiskunnan keskeisiin palveluihin.

4 Ahvenanmaan toimivalta

Ahvenanmaan itsehallintolain (1144/1991) 18 §:n mukaan maakunnalla on eräin rajoituksin lainsäädäntövaltaa asioissa, jotka koskevat elinkeinotoimintaa. Lain 27 §:n mukaan puolestaan valtakunnalla on lainsäädäntövaltaa asioissa, jotka koskevat kaupparenkulkua, ilmailua, standardisointia sekä valtion viranomaisten järjestysmuotoa ja toimintaa.

5 EU:n oikeuden mukainen oikeusperusta ja päätöksentekomenettely

Komissio katsoo, että Euroopan Unionilla on Euroopan unionin toiminnasta tehdyn sopimuksen (jäljempänä SEUT) 26 ja 114 artiklan nojalla oikeus toimia direktiivissä ehdotetussa asiassa. Edellä mainitun 26 artiklan mukaan unioni hyväksyy toimenpiteitä, joiden tarkoituksena on toteuttaa sisämarkkinat tai varmistaa niiden toiminta noudattaen asiaa koskevia perussopimusten määräyksiä. Saman artiklan 3 kohdassa todetaan neuvoston asettavan komission ehdotuksesta suuntaviivat, jotka ovat tarpeen tasapainoisen kehityksen takaamiseksi kyseisillä aloilla.

Mainitun 114 artiklan mukaan EU voi toteuttaa sisämarkkinoiden toteuttamista ja toimintaa koskevia toimenpiteitä jäsenvaltioiden lakien asetusten ja hallinnollisten määräysten lähentämiseksi. Komissio katsoo, että verkko- ja tietojärjestelmät helpottavat olennaisella tavalla vapaata liikkuvuutta ja rajat

ylittävien järjestelmien sietokyky ja vakaus ovat olennaisen tärkeitä sisämarkkinoiden moitteettomalle toiminnalle. Komission mukaan verkko- ja tietoturvan kansallisten valmiuksien, toimintamallien ja suojatason epätasaisuudesta johtuvat erot jäsenvaltioiden välillä johtavat esteisiin sisämarkkinoiden toiminnassa.

Komissio katsoo, että ehdotus on toissijaisuusperiaatteen mukainen, koska verkko- ja tietoturvan rajat ylittävän luonteen vuoksi toiminnan puute EU:n tasolla johtaisi tilanteeseen, jossa kukin jäsenvaltio toimisi yksinään ottamatta huomioon EU:n verkko- ja tietojärjestelmien keskinäisiä riippuvuussuhteita.

Komission mukaan ehdotus on myös suhteellisuusperiaatteen mukainen, koska jäsenvaltioihin kohdistuvat vaatimukset asetetaan minimitasolle, joka on tarpeen riittävän varautumistason saavuttamiseksi ja luottamukseen perustuvan yhteistyön harjoittamiseksi.

Ehdotuksen käsittely EU:n toimielimissä

Direktiiviehdotusta käsitellään EU:n parlamentissa, liikenne-, televiestintä ja energianeuvostossa sekä sen alaisessa televiestintä- ja tietoyhteiskuntatyöryhmässä.

6 Kansallinen valmistelu

Osapuolten kuuleminen

Liikenne ja viestintäministeriö on kuullut eri toimialoja erittäin laajasti direktiiviehdotuksesta tätä kirjelmää ja valtioneuvoston kantaa valmisteltaessa. Lukuisten EU-jaostojen puheenjohtajia ja sihteereitä pyydettiin arvioimaan, onko direktiiviehdotusta ja laadittua U-kirjelmän luonnosta tarpeen käsitellä jaostoissa kirjallisessa menettelyssä. Jaostot olivat oikeus- ja sisäasioiden jaosto (EU7), sisämarkkinat -jaosto (EU8), rahoituspalvelut ja pääomaliikkeet -jaosto (EU10), elinkeinopolitiikkajaosto (EU13), energia ja Euratom -jaosto (EU21), viestintäjaosto (EU19), liikennejaosto (EU22), terveysjaosto (EU33). Ehdotus on käsitelty ainakin oikeus- ja sisäasioiden jaoston, rahoituspalvelut ja pääomaliikkeet -jaoston sekä viestintäjaoston

kirjallisessa menettelyssä. Lisäksi ehdotusta on käsitelty terveys-jaoston (EU33) kokouksessa 25.2.2013. Lisäksi ehdotus ja U-kirjelmäluonnos on lähetetty tiedoksi valtioneuhallinnon tietoturvallisuuden johtoryhmälle ja kansallisen kyberturvallisuusstrategian valmistelleelle työryhmälle.

Liikenne- ja viestintäministeriö sai yhteensä 17 lausuntoa direktiiviehdotuksesta ja sitä koskeneesta U-kirjelmän luonnoksesta. Lausunnon antoivat: Asianajajaliitto, Elinkeinoelämän keskusliitto, Finanssialan keskusliitto, Toimihenkilökeskusjärjestö STTK, Finanssivalvonta, Huoltovarmuuskentrus, Keskuskaupakamari, Nasdaqomx (Pörssi), OP-Pohjola, Poliisihallitus, Telia Sonera Finland Oyj, Tietoliikenteen ja tietotekniikan keskusliitto Ficom ry, Työ- ja elinkeinoministeriö, Valtiovarainministeriön rahoitusmarkkinaosasto, Valtiovarainministeriön julkisen hallinnon ICT-toiminto sekä Viestintävirasto.

Lausunnoissa direktiiviehdotuksen tavoitteita pidettiin pääsääntöisesti perusteltuina ja kannatettavina. Lausunnoissa kiinnitettiin kuitenkin huomiota yleensäkin sääntelytarpeeseen sekä direktiiviehdotuksen tosiasialliseen tehokkuuteen julkilausuttujen tavoitteiden saavuttamiseksi. Edelleen lausunnoissa kiinnitettiin huomiota hallinnollisen taakan sekä taloudellisten kustannusten lisääntymiseen vaaraan erityisesti niiden toimijoiden osalta, jotka olisivat turvallisuusvaatimusten ja ilmoitusvelvollisuuden alaisia. Useissa lausunnoissa myös esitettiin vetoamus tietoturva-asioissa hyvin toimivan suomalaisen luottamukseen perustuvan yhteistyömallin ja tiedonvaihdon edellytysten turvaamiseksi yritysten ja Viestintäviraston välillä. Finanssialan toimijoiden lausunnoissa esitettiin näkemys, että finanssialan osalta vastuuviranomaisena tulisi olla Finanssivalvonta, joka muutoinkin vastaa alan riskien valvonnasta ja siihen liittyvien määräysten valvonnasta.

Komissiolle delegoidut toimivaltuudet herättivät huolta lausunnonantajissa. Osa lausunnonantajista katsoi, että delegoidun norminantovallan lisääminen aiheuttaisi merkittävää oikeudellista epävarmuutta ja että ehdotukseen sisältyvät ilmoitusvelvollisuudet tulisi määritellä jo direktiivissä selkeästi ja tarkkarajaisesti. Useissa lausunnoissa korostettiin sitä, että teknisten vähimmäisvaati-

musten määrittäminen tulisi perustua kansainvälisiin standardeihin. Direktiivin soveltamisalasta esitettiin sekä laajentavia että supistavia näkemyksiä. Useissa lausunnoissa esitettiin tarvetta tarkastella direktiiviehdotuksen suhdetta EU:ssa valmisteltavana olevaan henkilötietojen suojaa koskevaan tietosuoja-asetukseen.

7 Valtioneuvoston kanta

Valtioneuvosto kannattaa komission ehdotuksen tavoitetta verkko- ja tietoturvallisuuden korkean tason turvaamiseksi Euroopan Unionissa ja sen jäsenmaissa. Valtioneuvosto osallistuu hallitusohjelman mukaisesti aktiivisesti tietoverkkoturvallisuutta koskevaan kansainväliseen yhteistyöhön ja valtioneuvosto kannattaa sellaisia toimenpiteitä, jotka kannustaisivat kaikki jäsenvaltiot laatimaan strategiset tavoitteensa ja toimimaan yhteistyössä korkean tietoturvallisuuden ylläpitämiseksi ja tietoturvaloukkausten haitallisten vaikutusten torjumiseksi.

Tieto- ja viestintäteknologioista sekä niihin perustuvista tietojärjestelmistä ja palveluista tulee yhteiskunnan toiminnan kannalta yhä välttämättömämpiä. Niihin kohdistuvien uhkien rajat ylittävästä luonteesta johtuen Euroopan unionin jäsenmaiden välistä yhteistyötä tulee tiivistää ja kehittää edelleen.

Valtioneuvosto pitää perusteltuna, että kaikki jäsenvaltiot velvoitettaisiin määrittämään viranomaisvastuunsa ja perustamaan kansallisena tietotekniikan kriisiryhmänä toimiva CERT -ryhmä. Viranomaisten välisen keskinäisen yhteistyön kehittämiseksi on syytä luoda edellytyksiä tavalla, jossa eri viranomaisten lakisääteiset tehtävät ja vastuut säilyvät selkeinä.

Valtioneuvosto katsoo, että tietoturvallisuutta koskevan läpinäkyvyyden lisäämiseksi ja paremman tilannetietoisuuden muodostamiseksi on tärkeää kerätä ja jakaa tietoa sellaisista tietoturvaloukkauksista sekä niiden haitallisista vaikutuksista, jotka vaarantavat yhteiskunnan häiriötöntä toimivuutta. Tällaisesta sääntelystä on hyviä kokemuksia sähköisen viestinnän toimialalla, jonka keskeisimmät toimijat on lainsäädännössä veloitettu ilmoittamaan tietoturvaloukkauksista ja

häiriöistä luottamusta ja puolueettomuutta nauttivalle kansallisena tietoturvaviranomaisena toimivalle Viestintävirastolle. Näitä kokemuksia tulisi mahdollisuuksien mukaan hyödyntää myös muilla yhteiskunnan toimivuuden kannalta keskeisillä toimialoilla, joiden toiminta on riippuvaista sähköisistä tietojen viestintäpalveluista ja niiden häiriöttömyydestä. Samalla on kuitenkin huolehdittava siitä, ettei Suomessa hyvin toimivan tietoturvayhteistyön edellytyksenä olevaa yritysten ja viranomaisten välistä keskinäistä luottamusta vaaranneta tarpeettomasti eikä menettelyillä lisätä kenenkään hallinnollista taakkaa kohtuuttomasti.

Valtioneuvosto pitää tärkeänä, että kukin yhteiskunnan toimija kantaa itse vastuunsa omien tietojärjestelmiensä häiriöttömyydestä ja turvallisesta käytöstä. Tiedon suojaamisen tarpeet ja tietoturvaloukkausten haitalliset vaikutukset yhteiskunnassa vaihtelevat huomattavasti eri yrityksissä, toimialoilla ja eri jäsenvaltioissa. Sen vuoksi on tärkeää, että kansallisilla viranomaisilla säilyy tarkoituksenmukainen liikkumavara määrittää, millaisen ilmoituskynnyksen ylittävistä tapahtumista yritysten ja hallinnon tulisi ilmoittaa viranomaisille. Kansallisilla viranomaisilla

tulisi säilyttää tarkoituksenmukainen määrä harkintavaltaa rajat ylittävän tiedonvaihdon ja muiden tietoturvaan liittyvien toimenpiteiden osalta.

Valtioneuvosto pitää sisämarkkinoiden toimivuutta tärkeänä tavoitteena ja katsoo, että yhtenäinen eurooppalainen sääntely olisi omiaan edistämään luotettavien digitaalisten palvelujen ja sisämarkkinoiden kehittymistä EU:n alueella. Direktiivissä määriteltyjen toimialojen markkinat sekä julkishallinto ovat kuitenkin monilta osiltaan kansallisia, minkä vuoksi on tärkeää, että direktiiveissä otetaan riittävässä määrin huomioon kansallisten markkinoiden ja julkishallinnon erilaiset etenemisnopeudet ja sääntelytarpeet. Liian pitkälle viedystä harmonisoinnista voisi tulla kehityksen jarru, mikä ei edesauttaisi EU:n päämääräksi Lissabonin sopimuksessa julkilausuttujen tavoitteiden saavuttamisessa. Valtioneuvosto katsookin, että direktiivissä tulisi löytää tasapaino, joka mahdollistaa riittävän kansallisen liikkumavaran.

Valtioneuvosto katsoo myös, että komissiolle delegoitavien toimivaltuuksien tulisi olla tarkkarajaisia, oikeasuhtaisia, välttämättömiä ja hyvin perusteltuja.