

LIIKENNE- JA VIESTINTÄVALIOKUNNAN LAUSUNTO 11/2013 vp

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

Suurelle valiokunnalle

JOHDANTO

Vireilletulo

Eduskunnan puhemies on 22 päivänä maaliskuuta 2013 lähettänyt valtioneuvoston kirjelmän Euroopan parlamentin ja neuvoston direktiiviksi verkko- ja tietoturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella (U 13/2013 vp) käsiteltäväksi suureen valiokuntaan ja samalla määrännyt, että liikenne- ja viestintävaliokunnan on annettava asiasta lausuntonsa suurelle valiokunnalle.

Asiantuntijat

Valiokunnassa ovat olleet kuultavina

- neuvotteleva virkamies Timo Kievari, liikenne- ja viestintäministeriö
- EU-erityisasiantuntija Toivo Hurme, valtioneuvoston kanslia
- apulaisjohtaja Erka Koivunen, Viestintävirasto
- varautumispäällikkö Kari Wirman, FiCom.

Lisäksi kirjallisen lausunnon ovat antaneet

- Finanssivalvonta
- Terveiden ja hyvinvoinnin laitos (THL).

VALTIONEUVOSTON KIRJELMÄ

Ehdotus

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 tieto-

yhteiskunnan palvelun tarjoajat ja julkishallinnot ottamaan käyttöön riskinhallintakäytänteitä ja raporttoimaan ylläpitämiinsä keskeisiin palveluihin kohdistuvista merkittävistä tietoturvapoikkeamista.

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 turvallisuusviranomaisen (jäljempänä tietoturvaviranomainen), jonka tehtävänä olisi muun muassa valvoa direktiivin säännösten ja direktiivin nojalla säädettyjen 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 erikoistunut ryhmä, josta 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 tietoverkkorikosviraston 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 turvallisia tiedonvaihtokanavia pitkin. 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 rikos epäily, 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 käsillä olevaan 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 sovitaa yhteen yhteistyöverkoston viranomaisissa. Suunnitelmassa olisi lueteltu myös toimenpiteet verkko- ja tietoturvallisuutta koskevien har-

joitusten ja osaamisen kehittämiseksi (12 artikla).

Ehdotuksen mukaan komissio voisi solmia sellaisia sopimuksia unionin ulkopuolisten kolmansien maiden ja järjestöjen kanssa, jotka mahdollistaisivat niiden osallistumisen verkotuneiden 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 häiriöttömästi 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 sellaista 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. Tietotur-

vaviranomaisella 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 tällaisista standardeista (16 artikla).

Jäsenmaiden tulisi varmistaa, että direktiivin vastaisesta toiminnasta rangaistaisiin tehokkaila, oikeasuhtaisilla ja ennalta ehkäisevillä seuraamuksilla (17 artikla).

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 viestintätekniologioista sekä niihin perustuvista tietojärjestelmistä ja palveluista tulee yhteiskunnan toiminnan kannalta yhä välttämättömpiä. Niihin kohdistuvien uhkien rajat ylittävän luonteen vuoksi 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 velvoitettu 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 tieto- ja 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 häiriöttömästä ja turvalli-

sesta 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 saavuttamista. 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.

VALIOKUNNAN KANNANOTOT

Perustelut

Valiokunta pitää kannatettavana direktiivin tavoitetta turvata verkko- ja tietoturvallisuuden korkea taso Euroopan unionin alueella. Direktiivillä velvoitettaisiin jäsenvaltiot laatimaan kansallisesti tietoturvastrategia ja nimeämään kansallinen tietoturvaviranomainen. Valiokunta pitää erityisen hyvänä, että direktiiviehdotuksen

mukaan kaikkien jäsenvaltioiden tulisi perustaa tietoturvapoikkeamien ja -riskien selvittämiseen erikoistunut CERT-ryhmä (Computer Emergency Response Team).

Suomessa ensimmäinen kansallinen tietoturvastrategia laadittiin jo vuonna 2003, ja Viestintävirastolla ja sen CERT-FI-yksiköllä on jo vuosia ollut direktiivissä tarkoitettuja tietoturvaan

liittyviä tehtäviä. Viestintäviraston yhteyteen tullaan myös perustamaan uusi Kyberturvallisuuskeskus, ja kansallisen kyberturvallisuusstrategian visiona on, että Suomi on vuonna 2016 maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa. Valiokunnan käsityksen mukaan edellä mainituilla direktiivin ehdotuksilla ei näin ollen todennäköisesti olisi kovin huomattavia suoria vaikutuksia Suomen kannalta. Valiokunta kuitenkin korostaa, että tietoturvaohjeiden kansainvälisen luonteen vuoksi jokaisen jäsenmaan tietoturvan parantumisella on myös muita jäsenmaita hyödyttäviä vaikutuksia ja rajat ylittävien ongelmien hoitamisessa välttämättömän yhteistyön kehittäminen edellyttää, että kaikissa jäsenvaltioissa on selkeästi nimetyt kansalliset toimijat.

Direktiivissä ehdotetaan, että eräiden keskeisten alojen (rahoituspalvelut, liikenne, energia ja terveys) kriittisen infrastruktuurin ylläpitäjät sekä keskeisimmät tietoyhteiskunnan palvelun tarjoajat ja julkishallinnot veloitettaisiin toteuttamaan direktiivissä säädetyt tai sen nojalla määrätyt tietoturvan vähimmäisvaatimukset ja raporttoimaan merkittävistä niiden palveluihin kohdistuvista tietoturvaongelmista. Tältä osin direktiiviehdotus edellyttäisi toteutuessaan muutoksia kansalliseen sääntelyyn ja aiheuttaisi kustannuksia osalle uusien veloitteiden kohteista. Asiantuntijakuulemisessa on korostettu ehdotuksen taloudellisten vaikutusten arvioinnin ja huomioon ottamisen tarvetta ja sitä, että ehdotus ei saa lisätä kohtuuttomasti toimijoiden hallinnollista taakkaa. Valiokunta toteaa, että tämänkaltaisesta sääntelystä on varsin hyvin toimivia kokemuksia teleyritysten osalta. Valiokunta kuitenkin yhtyy erityisesti valtioneuvoston kantaan siitä, että direktiiviehdotus ei saa haitata Suomessa tällä hetkellä hyvin toimivaa ja nimenomaan keskinäiseen luottamukseen perustuvaa yhteistyötä yritysten ja Viestintäviraston tai muiden viranomaisten välillä. Vapaaehtoisuuteen ja tehokkaan yhteistyön kannalta välttämättömään luottamukseen perustuvien toimintamallien ja tietojenvaihdon toimivuutta ei tule

heikentää liian pitkälle menevällä pakottavalla sääntelyllä. Tämä koskee myös vakiintuneita kansainvälisen yhteistyön muotoja.

Valiokunta pitää tärkeänä, että direktiiviehdotuksessa komissiolle säädetyt tehtävät ja mahdollisesti delegoitavat toimivaltuudet määritellään täsmällisesti ja tarkkarajaisesti ja niiden sisältö ja tarve arvioidaan kaikilta osin huolellisesti. Valiokunta katsoo, että direktiivin säännösten ei tulisi olla liian joustamattomia ja jäsenvaltioille tulee mm. jäsenvaltioiden tämän hetkisistä tietoturvan toteuttamista koskevista eroista johtuen jättää riittävä liikkumavara tavoitteiden toteuttamisessa ja mm. tietoturvahäiriöitä koskevien ilmoitusvelvollisuuksien tarkemman määrittelyn osalta. Valiokunta pitää myös keskeisenä, että direktiivin valmistelussa huolehditaan tietosuojaan ja luottamuksellisen viestin suojaan liittyvien näkökohtien asianmukaisesta huomioon ottamisesta mm. tietoturvahäiriöiden selvittämiseen ja tietojen luovutusvelvollisuuksiin liittyen.

Valiokunta pitää jäsenvaltioiden välisen yhteistyön lisäämistä tärkeänä. Kansainvälinen tietojenvaihto on käytännössä välttämätöntä, mutta liian laajalla tietojen eteenpäin välittämisellä saattaa olla myös haitallisia vaikutuksia esimerkiksi siltä kannalta, miten halukkaita tietyn jäsenmaan yritykset ovat käytännössä toimittamaan tietoja viranomaisille. Tästä syystä valiokunta toteaa, että saattaisi olla paikallaan arvioida, tulisiko velvollisuus tietojen välittämiseen voida rajata esimerkiksi vain niihin muiden maiden viranomaisiin, joita uhkan arvioidaan koskevan, ja vain niihin tietoihin, jotka ovat välttämättömiä kyseisen uhkan torjumiseksi.

Valiokunta pitää erittäin hyvänä ja tärkeänä, että direktiivi asettaa vain tietoturvan vähimmäistason, ja sitä korkeampaa tasoa voidaan haluttaessa tavoitella kansallisesti joko vapaaehtoisin yhteistyömenettelyin tai tarvittaessa kansallisen sääntelyn keinoin. Valiokunta pitää myös olennaisena, ettei sääntelyn yhtenäistäminen EU-tasolla saa aiheuttaa paineita heikentää nykyisiä hyväksi koettuja tietoturvaa koskevia menettelyjä tai toimintamalleja.

Lausunto

Lausuntonaan liikenne- ja viestintävaliokunta ilmoittaa,

että se yhtyy asiassa valtioneuvoston kantaan korostaen edellä esitettyjä näkökohtia.

Helsingissä 24 päivänä huhtikuuta 2013

Asian ratkaisevaan käsittelyyn valiokunnassa ovat ottaneet osaa

pj.	Kalle Jokinen /kok	Johanna Ojala-Niemelä /sd
jäs.	Mikko Alatalo /kesk	Eila Tiainen /vas
	Ari Jalonen /ps	Ari Torniainen /kesk
	Jukka Kopra /kok	Reijo Tossavainen /ps
	Merja Kuusisto /sd	Mirja Vehkaperä /kesk
	Suna Kymäläinen /sd	vjäs. Reijo Hongisto /ps.

Valiokunnan sihteerinä on toiminut

valiokuntaneuvos Juha Perttula.