DITTMAR & INDRENIUS

Asianajotoimisto Oy

Jukka Lång, Partner
+358 9 681 70118
jukka.lang@dittmar.fi

LAUSUNTO

26.2.2020

Liikenne- ja viestintäministeriölle

LAUSUNTO SÄHKÖISEN VIESTINNÄN PALVELUISTA ANNETTUUN LAKIIN EHDOTETUSTA 5G-TEKNOLOGIAN TURVALLISUUTTA EDISTÄVISTÄ KEINOISTA

YLEISTÄ

Liikenne- ja viestintäministeriö on pyytänyt lausuntoja ehdotuksestaan uudeksi 244 a §:ksi lakiin sähköisen viestinnän palveluista ("SVPL") (917/2014). Dittmar & Indrenius Asianajotoimisto Oy ("Dittmar & Indrenius") pyytää edustamansa päämiehensä puolesta, että seuraavat näkökohdat otetaan jatkovalmistelussa huomioon.

TIIVISTELMÄ

Tässä lausunnossa tarkemmin kuvatulla tavalla:

1 Ehdotettu säännös edellyttää muutoksia, jotta säännökselle asetetut kansalliset ja EU-lainsäädännöstä seuraavat tavoitteet voidaan täyttää.

2 Lainsäädännön jatkovalmistelussa tulisi nykyistä tarkemmin huomioida Euroopan unionissa valmistellun Keinovalikoiman (*"EU Toolbox of risk mitigating measures/ Cybersecurity of 5G networks"*) määrittelemät tavoitteet ja keinot siten, että Suomen sääntely tulee paremmin vastaamaan muuta eurooppalaista sääntelyä.

3 Uutta sääntelyä ja valvontaa ei tulisi rajoittaa yksinomaan verkon kriittisiin osiin, vaan soveltamisalan tulisi noudattaa tarkemmin Keinovalikoiman lähtökohtia siten, että turvallisuutta voidaan edellyttää sekä arvioida laajemmin ja kokonaisvaltaisemmin.

4 Tavoitteisiin pääseminen edellyttää turvallisuutta koskevien vaatimusten ennakollista asettamista viestintäverkkolaitteille sekä riskien arvioimista jo ennen laitteen liittämistä yleiseen viestintäverkkoon, eikä pelkkää jälkikäteistä valvontaa voida pitää riittävänä.

5 Muitakin kuin teknisiä riskejä tulisi määrittää sääntelyssä ja sen perusteluissa tavalla, joka tuottaa selkeät arviointikriteerit, sillä toimivaltaisilla viranomaisilla on oltava riittävät toimivaltuudet reagoida myös yllättäen ilmeneviin ja luonteeltaan odottamattomiin riskeihin.

6 Uuden sääntelyn tulisi mahdollistaa riskien jatkuva arviointi ja niihin puuttuminen toimittajakohtaisesti ja toimitusketjujen näkökulmasta, ottaen huomioon etenkin korkeariskisiksi tunnistettavat laitteet ja toimittajat – riskiarviointi pelkästään yksittäisten laitteiden kautta ei ole riittävä eikä käytännössä toimiva valvontamekanismi.

7 Valmistellun säännöksen soveltaminen myös taannehtivasti, jo viestintäverkkoihin asennettujen laitteiden osalta lisäisi sen tuomaa turvallisuutta merkittävästi, ja on siten välttämätöntä.

TAUSTA JA ARVIOINNIN PERUSTEET

Suomessa on asetettu tavoite vahvistaa digitaalisaatiokehitystä tekemällä Suomesta 5G-teknologian kärkimaa.[1] 5G-teknologialla on merkittävä rooli lähitulevaisuuden kehityksessä. Se muun muassa mahdollistaa uudet palvelut ja ratkaisut useille yhteiskunnan kannalta keskeisille sektoreille kuten teollisuuteen, terveydenhuoltoon ja liikenteeseen. Se tarjoaa valtavan kapasiteetin siirtää dataa edullisesti ja mahdollistaa lähes reaaliaikaisen tiedonsiirron. Reaaliaikaisuus tarjoaa lukuisia mahdollisuuksia rakentaa uudenlaisia räätälöityjä palveluita robotiikan, tekoälyn, dataliiketoiminnan ja lisätyn todellisuuden tarpeisiin, niin yksityisellä kuin julkisella sektorilla.[2]

Digitalisoituva yhteiskunta ja sen toiminnan keskiössä olevat verkkopalvelut edellyttävät tarkoituksenmukaisia ja myös teknologisessa kehityksessä tehokkaita työkaluja tietoturvallisuuden ja ennen kaikkea kansallisen turvallisuuden varmistamiseksi.

[1] Liikenne- ja viestintäministeriö: Suomi tietoliikenneverkkojen kärkimaaksi – Digitaalisen infrastruktuurin strategia 2025, Liikenne- ja viestintäministeriön julkaisuja 10/2018.
[2] Liikenne- ja viestintäministeriö: 5G Momentum -hankkeen verkkosivusto.

Lainsäädännöllisiä keinoja valmisteltaessa on huomioitava muiden uhkien ohella Suomeen kohdistuva tiedustelutoiminta ja lisääntynyt kybervakoilu.[3] Suojelupoliisin tuoreen arvion mukaan ulkomaisten tiedustelupalveluiden kiinnostus Suomen kriittistä infrastruktuuria kohtaan on lisääntynyt[4].

Onkin selvää, että 5G-verkot muodostavat osan yhteiskunnan kriittistä infrastruktuuria, ja 5G-verkkojen turvallisuudella on erityisen tärkeä merkitys yhteiskuntamme ja taloutemme sekä Euroopan unionin ja jäsenvaltioiden itsemääräämisoikeuden turvaamisessa.[5] 5G-verkoilla on merkittävä vaikutus liiketoimintaympäristön ja uuteen teknologiaan nojaavien palveluiden kehittämisessä niin kuluttajien kuin yritystenkin kannalta. Myös viestinnän luottamuksellisuuden turvaaminen laajemmin on suojattava perusoikeutena niin lainsäädännön kuin viranomaistoiminnan tasolla.

On arvokasta, että liikenne- ja viestintäministeriössä valmistellaan lainsäädäntömuutoksia, joilla kuvattuihin haasteisiin pyritään vastamaan. Valmisteltavana oleva sähköisen viestinnän palveluista annettuun lakiin täydennettäväksi suunniteltu uusi 244 a § määrittelisi viestintäverkon kriittisissä osissa käytettäviin laitteisiin kohdistuvia vaatimuksia, ja 5G-teknologian käyttöönoton näkökulmasta sen on katsottava muodostavan merkittävää uutta sääntelyä verkkoinfrastruktuurin kannalta. Ehdotettu säännös on nähtävä myös yhteydessä tavoitteeseen kehittää Suomesta 5G-teknologian kärkimaa.

Infrastruktuurin kehittämistavoite kytkeytyy sekä teknologiakehityksen turvaamisen että turvallisuuden takaamisen tavoitteisiin. Kumpaakaan ei voi olla ilman toista, ja näiden välinen tasapainon toteutuminen on sääntelyratkaisuissa varmistettava.

Kuten ehdotetun uuden pykälän perusteluissa on huomioitu, viestintäverkkojen sääntely edellyttää käytännössä aina omaisuuden suojaan puuttumista. Perustuslakivaliokunnan käytännössä on hyväksytty rajoitukset, jos ne perustuvat lakiin ja ovat omistajan kannalta kohtuullisia.

Liikenne- ja viestintäministeriön perusteluissa kuvattu huomio siitä, että omaisuuden suojasta johtuen valmisteltavan säännöksen soveltamisalaa tulisi aina tulkita suhteellisuusperiaatteen mukaisesti mahdollisimman suppeasti ja rajoittaa tarkastelu pienimpään mahdolliseen osaan viestintäverkkoa, on perusteltu. Kuitenkaan suhteellisuusperiaatteen perusteella todettu lähtökohta ei anna

[3] Suojelupoliisi: Kansallisen turvallisuuden katsaus, 5.12.2019, s. 2.
[4] Suojelupoliisi: Kansallisen turvallisuuden katsaus, 5.12.2019, s. 2.
[5] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, s. 3.

perustetta säätää lainsäädännön tarkoituksiin ja muiden perusoikeuksien suojaamiseen nähden perusteettoman kapeaa soveltamisalaa. Turvallisuutta toteuttavista tarpeellisiksi havaittavista ja siten väistämättä omaisuuden suojaa rajoittavista rajoituksista on sen sijaan säädettävä lainsäädännön tasolla suhteessa suojattavaan perusoikeuteen, ottaen siis huomioon sekä turvallisuuden kannalta tärkeät perusoikeudet että myös niiden suojaamiseksi EU-tasolla määritellyt yhdenmukaiset linjat ja tavoitteet.

Keskeinen lähtökohta lainsäädäntötoimien arvioimisessa tulee olla Euroopan komission ja ENISA:n 5G-verkkojen ja -teknologian turvallisuusriskien hallitsemiseksi julkaiseman keinovalikoiman[6] ("Keinovalikoima") asettamien suositusten noudattaminen.

VIRANOMAISILLE EI SYNNY RIITTÄVIÄ EDELLYTYKSIÄ HUOLEHTIA VIESTINTÄVERKKOJEN TURVALLISUUDESTA 5G-TOIMINTAYMPÄRISTÖSSÄ

Nyt Suomessa voimassa oleva sääntely ja uuden säännöksen muodossa siihen ehdotetut muutokset eivät sellaisenaan antaisi lainsäädäntöä valvovalle keskeiselle viranomaiselle Liikenne- ja viestintävirastolle ("Traficom") riittäviä toimintavaltuuksia. Traficomilla ei ole eikä sille muodostuisi käytännön mahdollisuutta rajoittaa tietyn korkeariskisen toimittajan tai laitemallin käyttämistä muuten kuin yksittäisten viestintäverkkolaitteiden osalta. Näin ollen Traficomilla, tai muilla toimivaltaisilla viranomaisilla, ei olisi mahdollisuutta kattavasti tarkastella ja valvoa, mitä toimittajia viestintäverkon omistaja käyttää, eikä näihin liittyviä riskejä kansalliselle turvallisuudelle.

Tämä laitteita ja toimittajaketjuja koskeva ulottuvuus ei tule huomioiduksi myöskään verkkotoimilupia koskevan voimassaolevan sääntelyn myötä. Nykysääntelyssä turvallisuuden arviointitarve on huomioitu verkkotoimiluvan saamiseksi vertailevaan menettelyyn tai huutokauppaan osallistuvan verkko-operaattorin arvioinnissa. Laissa määritellyn mukaisesti, toimiluvan myöntämisestä voidaan poikkeuksellisesti poiketa

> *"jollei ole erityisen painavia perusteita epäillä toimiluvan myöntämisen vaarantavan ilmeisesti kansallista turvallisuutta".*[7]

On huomattava, että tämä kynnys on asetettu hyvin korkeaksi, ja sen soveltaminen edellyttäisi valtioneuvoston päätöksen. On oikeudellisesti hyvin vaativaa todeta kyseessä olevan "erityisen painavat perusteet" ja jonkin uhan olevan "ilmeinen". Arvioinnin

[6] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures.
[7] Laki sähköisen viestinnän palveluista 10 § ja 11 §.

kohteena oleva toimija on myös mahdollisesti väärä taho turvallisuuden arvioinnin kannalta, sillä verkkotoimilupa myönnetään teleyritykselle, joka voi harkintansa mukaan viestintäverkkoja toteuttaessaan käyttää erilaista verkkolaiteinfrastruktuuria.

5G-teknologian myötä verkkolaiteinfrastruktuuria koskeva ulottuvuus on aiempaa merkittävämpi. Nyt ehdotetun uuden säännöksen jättämät, tässä lausunnossa kuvaamamme, aukot johtaisivat väistämättä siihen, etteivät toimivaltaiset viranomaiset saisi riittäviä kyvykkyyksiä pystyäkseen kattavasti suojaamaan kansalaisten perusoikeutena turvattavaa viestinnän luottamuksellisuutta sekä kansallisesti merkitykseltään jatkuvasti kasvavaa viestintäverkkoinfrastruktuurin turvallisuutta. Sääntelyratkaisu jättäisi myös täyttämättä asian arvioinnin kannalta nähdäksemme keskeisen merkityksellisen EU-tasolla valmistellun Keinovalikoiman asettamat tavoitteet.

Keinovalikoima edellyttäisi kokonaisvaltaisempaa turvallisuusarviointia. Keinovalikoiman tavoitteena on ollut tunnistaa yhteisiä toimenpiteitä 5G-verkkoihin liittyvien keskeisten tietoturvauhkien hallitsemiseksi sekä ohjeistaa toimenpiteiden määrittämisessä. Tarkoituksena on ollut luoda kestävät puitteet sekä yhdenmukaiset toimintamallit 5G-verkkojen turvallisuuden varmistamiseksi EU-alueella.

Tarkastellessaan voimassaolevaa lainsäädäntöä Keinovalikoiman näkökulmasta liikenne- ja viestintäministeriö todennut, että lainsäädäntö vastaa varsin hyvin keinovalikoimassa esitettyihin vaatimuksiin.[8] Ainoa varsinaista muutosta edellyttävä kokonaisuus on liikenne- ja viestintäministeriön arvion mukaan verkon kriittisempien osien suojaaminen.

Suorittamamme vertailun ja analyysin perusteella liikenne- ja viestintäministeriön arvio ei kestä kriittistä tarkastelua, erityisesti huomioiden EU-tasolla korostettu turvallisuusuhkien käsittelytarve ja etenkin Keinovalikoiman mukaisten toimenpiteiden käytäntöön saattaminen. Ehdotettu säännös ei esimerkiksi mahdollistaisi korkeariskisten toimijoiden rajoittamista, vaan keskittyy yksittäisiin viestintäverkkolaitteisiin.

Korkeariskisiä toimittajia ei mainita ehdotetussa säännöksessä tai voimassaolevassa laissa, eikä ehdotettu säännös täytä Keinovalikoiman mukaisia toimenpiteitä tai säännökselle laajemmin Keinovalikoiman kautta asetettuja tavoitteita. Keinovalikoiman mukaisesti viranomaisten on arvioitava tiukasti kaikkien merkityksellisten

[8] Liikenne- ja viestintäministeriön sähköisen viestinnän palvelulain uudistuksen seurantaryhmän kokous 14.2.2020 (tilaisuuden tallenne jaettu verkossa: https://www.youtube.com/watch?v=t8AsQoPCKk4).

toimittajien riskiprofiileita ja sovellettava tarpeellisia rajoituksia.[9] Kokonaisvaltaisempi arviointi olisi tarpeen toimittajien ja niihin liittyvien riskien arvioimiseksi Keinovalikoimassa suositellulla tavalla.

Jos Suomen lainsäädäntö rajoitettaisiin tältä osin soveltumaan ehdotetun pykälän mukaisesti vain laitteisiin, se ei noudattaisi Keinovalikoiman mukaista vaatimusta arvioida riskiprofiilia kaikkien toimittajien osalta. Esimerkiksi mikäli toimittajan laite määrättäisiin poistettavaksi, voisi sama toimittaja, ja mahdollisesti jopa sama laite, silti myöhemmin tai samanaikaisesti toisaalla olla osa 5G-toimitusketjua. Samoin vaikka yksittäisen toimittajan laite määrättäisiin poistettavaksi, ei Traficomilla olisi mahdollisuutta ehdotetun säännöksen alla määrätä rajoituksia esimerkiksi toimittajan kanssa saman lainsäädännön alla toimivan ja tämän kanssa samaan konserniin kuuluvan yhtiön laitteiden osalta. Näin ollen jälkikäteinen, ainoastaan laitteisiin kohdistuva arviointi ei turvaisi kansallista turvallisuutta tai täyttäisi Keinovalikoiman mukaisia toimenpiteitä riittävällä tasolla.

Lisäksi Keinovalikoima huomioiden Suomen lainsäädännön tarkastelemisessa 5G-verkkoihin kohdistuvien riskien hallitsemiseksi tulisi arvioida myös muita mahdollisia toimenpiteitä, jotka eivät ole suoraan sidoksissa ehdotettuun säännökseen ja joita ei näin ole tarkemmin arvioitu tässä lausunnossa. Viranomaisten tulisi esimerkiksi voida vaatia teleoperaattoreita toimittamaan yksityiskohtaisia tietoja suunnitelmistaan 5G -laitteiden hankkimiseksi ja toimittajien osallistumiseksi[10]. Voimassaoleva sääntely ehdotetuin muutoksin ei myöskään muilta kuin ehdotetun säännöksen tarkoitusten osalta riittäisi täyttämään Keinovalikoiman toimittajien ja toimitusketjujen valvonnalle asettamia vaatimuksia,[11] tai vastaisi useissa muissa EU-maissa Keinovalikoiman huomioivia malleja.[12]

KRIITTISTEN OSIEN MÄÄRITELMÄ RAJOITTAA VALVONTAMAHDOLLISUUKSIA

Ehdotetun säännöksen mukainen kriittisten osien määritelmä on perusteettoman kapea eikä vastaa Keinovalikoiman mukaista määritelmää. Keinovalikoimassa edellytetään toimenpiteiden, kuten toimittajaketjun valvonnan, kohdistamista verkon arkaluonteisimpiin ja tärkeimpiin osiin (eng. "*sensitive assets*" ja "*key assets*"), eikä toimenpiteitä rajoiteta pykäläluonnoksessa suunnitellulla tavalla

[9] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, toimenpide SM03, s. 21.
[10] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, s. 20.
[11] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, s. 21.
[12] Esimerkiksi Hollannissa lainsäädäntö mahdollistaa huomattavasti laajemmin toimittajaketjun arvioinnin sen antaessa viranomaisille mahdollisuuden määrätä vain sellaisten toimittajien käyttämistä, joita ei ole katsottu epäluotettaviksi.

verkon kriittisiin osiin[13]. Näitä merkityksellisiä ja arkaluonteisia osia eivät 5G-teknologian myötä ole enää yksinomaan verkon ydinosat (eng. "*core*"), vaan verkon toiminnallisuuksien siirtäminen lähemmäksi loppukäyttäjiä johtaa verkon kriittisten ja tosiasiallisesti keskeisten piirteiden siirtymiseen *core*-verkosta myös muualle verkkoon, tietyissä tilanteissa jopa loppukäyttäjälaitteisiin. Sivusta suoritetussa arvioinnissa näitä verkon ydinosista etäämmällä olevia toiminnallisuuksia on kuitenkin vaikeaa hahmottaa ja tunnistaa verkon kriittisiksi osiksi, ja onkin hyvin suuri riski siitä, että sääntelyn sitominen yksinomaan tähän termiin johtaisi viranomaispuuttumisen tosiasiallisten mahdollisuuksien perusteettomaan kaventumiseen ja lainsäädännön tavoitteiden toteutumatta jäämiseen.

Ehdotetun säännöksen mukainen määritelmä poikkeaisi siis Keinovalikoiman mukaisesta EU-tason lähtökohdasta, eikä toteuttaisi sen mukaista tarkoitusta. Keinovalikoiman mukainen määritelmä ei näkemyksemme mukaan rajoittaisi omaisuudensuojaa ehdotettua säännöstä laajemmin, eikä siis nähdäksemme ole perusteita poiketa Keinovalikoiman mukaisesta linjasta.

Kansallisen määritelmän ja tästä seuraavan toimenpiteiden soveltamisalan ei tulisi olla kapeampi kuin Keinovalikoimassa ja EU-tasolla määritetyssä yhdenmukaisessa linjassa.

Jälkimmäisen osalta on tärkeää huomioida Keinovalikoiman lisäksi Euroopan unionin Neuvoston päätelmät 3.12.2019 5G:n merkityksestä Euroopan taloudelle ja tarpeesta lieventää 5G:hen liittyviä turvallisuusriskejä[14]. Päätelmän mukaisesti Neuvosto:

"*10* *WELCOMES the ongoing joint European efforts on safeguarding the security of 5G networks based in particular on the Commission Recommendation on Cyber Security of 5G Networks and STRESSES the importance of a coordinated approach and effective implementation of the Recommendation in order to avoid fragmentation in the Single Market.*

[…]

12 *EMPHASISES that the technological changes introduced by 5G will increase the overall attack surface and require particular attention to the risk profiles of individual suppliers.*

[13] Kts. esim. Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, s. 20 & 39-40.

[14] Euroopan unionin neuvoston lehdistötiedote 3.12.2019 *5G-teknologian merkitys ja turvallisuusriskit – neuvostolta päätelmät* (https://www.consilium.europa.eu/fi/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/).

13 *STRESSES that in addition to the technical risks related to cybersecurity of 5G networks, also non-technical factors such as the legal and policy framework to which suppliers may be subject to in third countries, should be considered.*

[…]

19 *EMPHASISES that 5G and other related electronic communications networks need to be protected continuously across their entire lifecycle to cover the whole supply chain and all relevant equipment.*"[15]

Vertailun vuoksi Ruotsin vastaavassa ehdotetussa sääntelyssä (2019/20:15) viitataan riskiarviointivelvoitteen osalta suoraan myös toimittajiin. Kyseisen ehdotetun säännöksen perusteluiden mukaisesti:

> *"Det bör också vara möjligt att t.ex. utesluta komponenter, leverantörer eller servicepersonal som inte håller en tillräckligt hög säkerhetsnivå."*[16]

Myös useat muut jäsenvaltiot, kuten Ranska, ovat ottaneet tarkemmin Keinovalikoiman mukaisen ja keskenään yhdenmukaisemman lähestymistavan uuden sääntelyn soveltamisalan määrittelyyn.

Ymmärrämme, että kriittisten osien määrittely on käytännössä haastavaa, ottaen huomioon 5G -teknologian erityispiirteet, ja aiheesta käydäänkin EU-alueella laajalti keskustelua. Ehdotetun säännöksen perusteluissa viitataan tältä osin omaisuuden suojan tuomiin rajoituksiin, ja todetaan, että säännöksen soveltamisalaa tulisi aina tulkita suhteellisuusperiaatteen mukaisesti mahdollisimman suppeasti rajoittaen tarkastelu pienimpään mahdolliseen osaan viestintäverkkoa. Arviomme mukaan Keinovalikoiman mukainen määritelmä ei kuitenkaan rajoittaisi omaisuudensuojaa suhteellisuusperiaatteen vastaisesti.

Ehdotettu määräyksenantovaltuutus Traficomille on näkemyksemme mukaan perusteltu ja tarpeellinen. Traficomilla on oltava mahdollisuus antaa tarkempia määräyksiä kriittisten osien määrittelystä, sillä näiden säätäminen lailla ei ole käytännössä perusteltua. Kriittisten osien tarkempi määrittely määräyksessä, tai laissa, ei kuitenkaan käytännössä ratkaise yllä kuvattuja haasteita.

[15] Euroopan unionin Neuvoston päätelmät 5G:n merkityksestä Euroopan taloudelle ja tarpeesta lieventää 5G:hen liittyviä turvallisuusriskejä, 3.12.2019.
[16] Regeringens proposition 2019/20:15 Skydd av Sveriges säkerhet vid radioanvändning, 19.9.2019 s. 29.

Traficomilla tulisi joka tapauksessa olla lakiin perustuva valtuus kieltää verkkolaitteen käyttö myös muissa kuin viestintäverkon kriittisissä osissa, mikäli turvallisuusarvioinnin perusteella voitaisiin todeta, että myös näihin osiin liittäminen vaarantaisi kansallisen turvallisuuden. Käytännössä muussa tapauksessa jäisi aina riski siitä, että myös muihin kuin kriittisiksi määriteltyihin osiin liitettävän verkkolaitteen vaarantaessa kansallisen turvallisuuden, asiaan ei voida puuttua tehokkaasti.

SÄÄNNÖKSEN TAVOITTEITA EI OLE MAHDOLLISTA SAAVUTTAA AINOASTAAN JÄLKIKÄTEISELLÄ VALVONNALLA

Ehdotetussa muodossa säännös mahdollistaisi ainoastaan jälkikäteisen puuttumisen kansallista turvallisuutta vaarantavien viestintäverkkolaitteiden käyttämiseen.

Verkkotoimiluvan edellytysten arvioinnin yhteydessä tarkastellaan myös toimiluvan mahdollisia vaikutuksia kansalliseen turvallisuuteen. Kuten edellä (s. 4) todettu, kynnys on tältä osin kuitenkin korostuneen korkea, eikä arviointi kohdistu kattavasti Keinovalikoimassa esitettyihin keinoihin. Lisäksi turvallisuutta vaarantavat seikat saattavat muodostua tai ilmetä vasta myöhemmin, kun uusia toimittajia tai viestintäverkkolaitteita lisätään.

Ennakollisen hyväksynnän puuttuessa voisivat viestintäverkon omistajat liittää verkkoonsa aiemmin kiellettyjä viestintäverkkolaitteita tai hankkia laitteita toimittajilta, joiden on aiempien arviointien yhteydessä katsottu vaarantavan kansallista turvallisuutta. Tämä sekä vaarantaisi kansallisen turvallisuuden ehdotetun säännöksen tavoitteiden vastaisesti että johtaisi mahdollisesti turhiin investointeihin viestintäverkon omistajan osalta.

Ennakkohyväksynnän puuttuminen johtaisi myös tältä osin siihen, ettei Suomen sääntelyllä voitaisi täyttää Keinovalikoiman mukaisia toimenpiteitä ja tavoitteita.

Yllä kuvattujen ennakollisen hyväksynnän ja arvioinnin puuttumisen tuomien riskien rajoittamiseksi suosittelemme seuraavien toimintamallien harkitsemista:

(i) Traficom laatii listan[17] laitteista, jotka sisältävät mahdollisesti korkean riskin ja jotka edellyttävät ennakkohyväksyntää[18];

[17] Listan laatimisessa on huomioitava muun muassa Keinovalikoiman mukaiset kriittisten ja arkaluonteisten verkkojen määritelmät.
[18] Vastaavan kaltaisesta ennakkohyväksyntää koskevasta mallista on säädetty esimerkiksi Ranskassa.

(ii) tunnistettujen korkean riskin toimittajien käyttäminen kielletään ennakolta sekä toteutetaan muut Keinovalikoiman toimenpiteen SM03 mukaiset toimet; ja/tai

(iii) Traficomille annetaan valtuus määrätä ennakollinen kielto käyttää tiettyjä viestintäverkkolaitetta tai -toimittajia[19].

VERKKOLAITTEEN POISTAMISEN EDELLYTYKSET OVAT EPÄSELVÄT

Muita kuin teknisiä riskejä ei arvioida kattavasti

Ehdotetun säännöksen perusteluiden mukaan kansallisen turvallisuuden vaarantuminen voi tarkoittaa esimerkiksi

> "*henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavaa toimintaa, vieraan valtion toimintaa, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille taikka ulkomaalaista tiedustelutoimintaa*".

Ehdotettu muotoilu ei nähdäksemme kuitenkaan toisi mahdollisuutta ottaa kattavasti huomioon vieraan valtion toimintaa tai ulkomaalaista tiedustelutoimintaa tilanteessa, jossa tarkasteltavana olevan viestintäverkkolaitteen ei voitaisi osoittaa vaarantavan kansallista turvallisuutta, mutta olosuhteet muilta osin osoittaisivat, että viestintäverkkolaitteen liittäminen saattaisi vaarantaa kansallisen turvallisuuden.

Vertailussa on myös huomioitava, että Keinovalikoiman mukaisesti muita kuin teknisiä riskejä voivat olla, muun muassa, 5G-toimitusketjuihin liittyvät riskit, ja toimittajakohtaisessa arvioinnissa olisi kiinnitettävä huomiota toimittajaa sitovaan kolmannen maan lainsäädäntöön.[20] Keinovalikoimassa tehdyn linjauksen taustalla on tunnistettu riski siitä, että kolmannen maan lainsäädäntö saattaa sisältää velvoitteita, joiden vaikutuksesta Suomen lainsäädännön viestintäverkkojen käyttäjille tarjoama suoja ja tietoturvallisuus tosiasiassa vaarantuvat, ja tällaisen tiedon ilmi tuleminen tai vahvistuminen olisi seikka, joka olisi tällöin voitava ottaa huomioon viranomaisen turvallisuusarvioinnissa.

[19] Vastaavan kaltainen ennakkokielto on mahdollista esimerkiksi Ruotsin ehdotetun vastaavan lain mukaisesti.
[20] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, s. 42–43.

Lisäksi, mikäli kriteereitä ja toimittajakohtaisia vaatimuksia ei Suomessa määritellä tarkemmin lainsäädännössä tai sen perusteluissa, olisi valvontapäätöksen kohteella mahdollisuus vedota selkeiden vaatimusten puuttumiseen sekä siihen, ettei lainsäädäntö ole ollut vaadittavan tarkkarajaista.

Näin ollen säännöksen perusteluissa ja Traficomin määräyksissä olisi kiinnitettävä erityistä huomiota siihen, että niissä huomioitaisiin myös tilanteet, joissa toimittajaa sitova kolmannen maan laki edellyttää toimintoja, jotka vaarantavat kansallisen turvallisuuden.[21]

Toimittajakohtaisia riskejä ei oteta kattavasti huomioon

Toimittajakohtaisten riskien huomioon ottaminen ei olisi ehdotetun säännöksen perusteella mahdollista. Tarkastelu kohdistuisi ainoastaan viestintäverkkolaitteisiin, ei niiden toimittajaan.

Näin ollen, vaikka Euroopan unionissa on valmisteltu ja keskusteltu yhdenmukaisesta varautumisesta 5G -verkkoon kohdistuviin uhkiin, Suomi ei voisi estää yksittäisen toimittajan viestintäverkkolaitteiden liittämistä verkon kriittisiin osiin, vaikka kyseinen toimittaja olisi muiden jäsenvaltioiden valvontatoimien perusteella todettu olevan korkeariskinen.

EU:ssa linjatun Keinovalikoiman mukaisesti toimittajien riskiprofiili tulisi arvioida ja korkeariskisiin toimittajiin tulisi soveltaa rajoituksia kriittisten toimintojen suojaamiseksi seuraavasti:[22]

> *"- Establish a framework with clear criteria, taking into account the risk factors identified in paragraph 2.37 of the EU coordinated risk assessment34 and adding country-specific information (e.g. threat assessment from national security services, etc.), for national competent authorities and MNOs to:*
>
> *- Perform rigorous assessments of the risk profile of all relevant suppliers at national level and/or EU level (for example jointly with other MS or other MNOs);*
>
> *-Based on the risk profile assessment, apply restrictions- including necessary exclusions to effectively mitigate risks- for key assets defined as critical or sensitive in the EU coordinated risk assessment report (e.g. core network functions, network*

[21] Ehdotetun säännöksen perusteluissa viitataan ulkomaiseen tiedustelutoimintaan, mutta viittaus on näkemyksemme mukaan käytännön soveltamisen kannalta liian yleisellä tasolla.
[22] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, toimenpide SM03, s.21.

management and orchestration functions, and access network functions);.

- Take steps to ensure that MNOs have adequate controls and processes in place to manage potential residual risks, such as regular supply chain audits and risk assessments, robust risk management, and/or specific requirements for suppliers based on their risk profile."

Suomessa voimaansaatettava säännös tulisi laatia tavalla, joka mahdollistaa myös korkean riskin toimittajien huomioimisen. Arvioinnissa tulisi Keinovalikoima huomioiden[23] olla mahdollista ottaa huomioon esimerkiksi kolmansien maiden lainsäädännön asettamat toimittajaa sitovat velvoitteet.[24]

Pidämme valitettavan mahdollisena, että nyt ehdotetun muotoilun perusteella riskeihin puuttuminen jäisi tosiasiassa käytännössä pieneksi. Säännöksen ehdotettu muotoilu jättää puuttumisen kynnyksen korkeaksi ja valtaosin Traficomin virkamiesten harkittavaksi yksittäistapausten kautta. Toimittajakohtaisten riskien arviointi jälkikäteisesti ilman selkeää mallia jättäisi mahdollisesti jopa kauppapoliittisesti ja yhteiskunnallisesti merkittävien päätösten tekemisen Traficomin, ja sen yksittäisten virkamiesten, vastuulle yksittäisten laitteiden arvioimisen yhteydessä.

Lisäksi, ehdotettu säännös mahdollistaisi vain yksittäisten viestintäverkkolaitteiden arvioinnin, mikä edellyttäisi viranomaisilta käytännössä aina tapauskohtaista harkintaa. Ennakkohyväksynnän vaatimus tai muiden ennakollisten toimien säätäminen parantaisi viranomaisten valvontamahdollisuuksia ja antaisi osaltaan tarpeellisen liikkumavaran tilanteessa, jossa muuttuvan turvallisuuspoliittisen tilannekuvan myötä viranomaiset saisivat uutta tietoa uhista ja toimittajista.

Traficomilla on arviomme mukaan voimassaolevan sääntelyn perusteella lähtökohtaisesti riittävät tiedonsaantioikeudet viestintäverkon omistajalta. Pyydämme kuitenkin kiinnittämään valmistelussa huomiota siihen, että tiedonsaantioikeuksien olisi mahdollistettava myös toimittajien ja toimitusketjujen valvonta kattavasti.

[23] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, s. 42.

[24] "*Kriittisen infrastruktuurin päätyminen kybervakoilua tai -vaikuttamista aktiivisesti harjoittavan valtion hallintaan aiheuttaa uhkan kansalliselle turvallisuudelle jo ennen kuin vakoilua harjoittava valtio päättää käyttää voimaansa.*" (Suojelupoliisi: Kansallisen turvallisuuden katsaus, 5.12.2019).

Yllä kuvattujen haasteiden rajoittamiseksi Traficomilla tulisi olla selkeät kriteerit toimittajien ja toimitusketjujen arviointiin, joka huomioisi myös toimittajakohtaiset heikkoudet ja riskit, kuten:

(i) riskit kolmannen maan vaikutuksesta ja toimittajan riippuvuudesta kolmanteen maahan;

(ii) toimittajaa sitovat suorat lainsäädännölliset velvoitteet; sekä

(iii) operationaaliset riskit.

Pidämme muiden jäsenvaltioiden käynnissä olevat lainsäädäntötoimet huomioiden todennäköisenä, että suurimmalla osalla muita jäsenvaltioita on muodostumassa huomattavasti paremmat edellytykset ottaa yllä kuvatut seikat huomioon arvioinnissa, kuin mitä Suomen viranomaisilla olisi ehdotetun säännöksen ja voimassaolevan lainsäädännön alla.

Yllä kuvattujen, Keinovalikoiman mukaisten, seikkojen huomioon ottamatta jättäminen johtaisi käytännössä siihen, että Suomi soveltaisi EU-tasolla yhdenmukaistettuja keinoja yleisestä EU-tason linjasta poiketen.

Pidämme perusteltuna määräyksenantovaltuutuksen antamisen harkitsemista Traficomille kriittisten osien määrittelyn lisäksi myös toimittajien arvioinnin sekä toimittajien toimintaa ja valintaa koskevien kriteerien ja vaatimusten osalta.

Lisäksi olisi tarpeen harkita sen nimenomaista mahdollistamista, että luonnolliset- ja oikeushenkilöt voisivat ilmoittaa Traficomille kansallista turvallisuutta vaarantavista laitteista. Vaikka ehdotettu sääntely ei sinänsä estäisi tällaista, tarkentaisi tällainen lisäys osaltaan Traficomin tutkintavaltuuksia.

TAANNEHTIVA SOVELTAMINEN TURVALLISUUDEN KANNALTA VÄLTTÄTÖNTÄ

Mikäli ennen ehdotetun säännöksen voimaantuloa viestintäverkkoon liitetyn viestintäverkkolaitteen havaittaisiin vaarantavan kansallisen turvallisuuden, Traficomilla ei olisi mahdollisuutta määrätä laitteen poistamista. Ehdotettu säännöstä sovellettaisiin sen nimenomaisen voimaantulosäännöksen mukaisesti ainoastaan lain voimaantulon jälkeen viestintäverkoissa käyttöön otettaviin viestintäverkkolaitteisiin.

Mikäli säännöstä ei sovellettaisi taannehtivasti, jäisivät sen vaikutukset merkittävästi pienemmiksi kuin, jos viestintäverkon turvallisuuden takaamiseksi tarpeelliset säädökset saatettaisiin yleisesti voimaan.

On ymmärrettävää, että ehdotetulla valinnalla vaikutettaisiin omaisuudensuojaan, mutta omaisuudensuoja ei näkemyksemme muodostaisi estettä taannehtivalle soveltamiselle, jolla pyritään turvaamaan muiden perusoikeuksien toteutumista. Yksittäisiä viestintäverkkolaitteita ei ole ennen tarkasteltu viranomaisten toimesta ehdotetun säännöksen kaltaisella tavalla, eikä niiden käyttöönotto ole edellyttänyt erillistä viranomaislupaa. Viestintäverkon omistajan ei lähtökohtaisesti tulisi katsoa saaneen perusteltujen odotusten suojaa sellaisten laitteiden käyttämiseksi, joiden myöhemmin katsotaan vaarantavan kansallisen turvallisuuden, ottaen huomioon etenkin se seikka, että verkkotoimilupaa ei olisi myönnetty, mikäli toimiluvan myöntäminen olisi vaarantanut ilmeisesti kansallista turvallisuutta.[25]

Näin ollen pidämme ehdotetun säännöksen soveltamista myös taannehtivasti perusoikeuksien turvaamisen näkökulmasta sekä oikeasuhtaisena (ottaen huomioon omaisuudensuojan rajoitukset) että välttämättömänä (ottaen huomioon kansallisen turvallisuuden ja viestinnän luottamuksellisuuden turvaamisen). Näkemyksemme mukaan suositeltavin toimintamalli olisi, että ehdotettua säännöstä täsmennettäisiin niin, että mikäli Traficom antaa poistamismääräyksen tietyn laitteen osalta, muiden viestintäverkon omistajien on poistettava laite vastaavilta osin siitä riippumatta, milloin laite on liitetty viestintäverkkoon.

Aiemmin kuvaamallamme tavalla ennen säännöksen soveltamista viestintäverkkoon liitettyjen laitteiden turvallisuutta ei voida katsoa jo arvioidun vain sillä perusteella, että kansallista turvallisuutta koskevat näkökohdat on huomioitu verkkotoimilupaprosessissa. Prosessissa ei huomioida kattavasti toimitusketjuihin ja korkeariskisiin toimittajiin liittyviä riskejä. Näin ollen taannehtivaa soveltamista vastaaviin vaikutuksiin ei päästäisi voimassaolevan sääntelyn alla.

MUUTOKSENHAUN VAIKUTUKSET ON HUOMIOITAVA KÄYTÄNNÖN SOVELTAMISESSA

Säännöksessä on ehdotettu, että Traficomin säännöksen nojalla tekemästä valvontapäätöksestä voisi valittaa hallinto-oikeuteen. SVPL:n 43 luvun 344 §:n mukaisesti Traficom voi päätöksessään ilmoittaa, että sitä on noudatettava muutoksenhausta huolimatta, jollei hallinto-oikeus toisin määrää.

[25] Tältä osin on huomattava, että vaikka aiemmin lausunnossa kuvaamallamme tavalla toimiluvan yhteydessä suoritettava arviointi ei ole riittävä uhkien torjumiseksi, on toimiluvan haltijan tullut käsittää, ettei kansallista turvallisuutta vaarantavia laitteita voida käyttää. Traficomin päätös tietyn laitteen kansallista turvallisuutta vaarantavasta vaikutuksesta ei siis tarkoittaisi viranomaismääräyksen tai lainsäädännön muuttamista perusteltujen odotusten vastaisesti, vaan jo aiemmin kielletyn toiminnan luonteen vahvistamista.

Mahdollisen muutoksenhaun näkökulmasta olisi säännöksen valmistelemisessa kiinnitettävä aiemmin tässä lausunnossa kuvaamallamme tavalla huomiota säännöksen muotoiluun, jotta epäselviin vaatimuksiin perustuvat virheelliset päätökset ja niitä seuraavat valitukset voidaan ehkäistä ennalta.

Päätöksen luonne huomioiden pidämme säännöksestä ja SVPL:n voimassaolevasta muodosta seuraavaa muutoksenhakumallia perusteltuna. Traficomin on kuitenkin yksittäisissä valvontapäätöksissään tärkeää kiinnittää erityistä huomioita muutoksenhaun vaikutuksiin ja tarpeeseen määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta.

LOPUKSI

Kokonaisuutena tarkastellen pidämme ehdotettua säännöstä tarpeellisena ja erityisen merkityksellisenä Suomeen ja 5G-verkkoihin kohdistuvien uhkien torjumiseksi. Säännöksen huolellisen valmistelemisen lisäksi myös sitä soveltavilla viranomaisilla on tärkeä rooli uhkien torjumisessa, minkä vuoksi korostamme säännöksen huolellisen perustelemisen merkitystä.

Helsingissä 26. päivänä helmikuuta 2020

DITTMAR & INDRENIUS

Jukka Lång
Asianajaja, Helsinki