9.3.2022

Eduskunta
Liikenne- ja viestintävaliokunta

VNS 11/2021 vp Valtioneuvoston selonteko tiedustelulainsäädännöstä / Asiantuntijapyyntö

Lausunto: Valtioneuvoston selonteko tiedustelulainsäädännöstä

Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Tässä lausunnossa huomio kohdistetaan yksinomaan *digitaaliseen toimintaympäristöön (ml. tietoliikenne)*.

Lähtökohtaisesti tiedusteluviranomaisilla tulee olla riittävät toimivaltuudet yhteiskunnan turvallisuusintressien suojaamiseen myös digitaalisessa ympäristössä. Tähän liittyen **tiedustelutoiminnan kytkeminen Suomen kansallisen turvallisuuden vahvistamiseen ja kriittisen infrastruktuurin ja huoltovarmuuden piirissä oleviin sektoreihin tulisi kyberturvallisuuden kehittämisen kannalta olla aiempaa selkeämpää.**

Tiedustelulainsäädäntöä koskevaa lainsäädäntöä laadittaessa elinkeinoelämän piirissä pidettiin perusteltuna, että viranomaisilla tulee olla selkeästi säädetyt mahdollisuudet tarpeellisten ja oikeasuhtaisten tiedustelutoimivaltuuksien käyttöön digitaalisessa ympäristössä. Samoin korostettiin, että **viranomaisten toimivaltuuksien käytön *ei tule heikentää yritysten kilpailukykyä tai toimintamahdollisuuksia***, vaan niiden tulee olla sopusoinnussa elinkeinopoliittisten kysymysten kanssa. Tämä lisäksi korostettiin hyvien valvontamekanismien ja jatkuvan vaikutusten seurannan merkitystä.

Kyberalalla ei ole yksityiskohtaisia tietoja sääntelyn vaikutuksista esimerkiksi yrityssalaisuuksien suojaan, Suomen kilpailukykyyn, uuden liiketoiminnan syntyyn tai tutkimus- ja kehitystoimintaan. ***Digitalisaatiosta johtuvista syistä yrityssalaisuuksien sekä muun liiketoimintaa koskevan tiedon luottamuksellisuus on nykyisellään kuitenkin yritysten elinehto. Oikeushenkilöitä koskevan luottamuksellisen viestinnän suojaa koskevan oikeuden merkitys on kasvanut entisestään sitten tiedustelulakien voimaantulon.*** Tähän vaikuttaa erityisesti tietoliikenteen ja datan jakaminen yli valtionrajojen (mm. pilviteknologian yleistyminen). Perusoikeudet ja lainsäädännön takeet toimintaympäristön luottamuksellisuudesta sekä viranomaisten toiminnasta lisäävät luottamusta digitaalisessa ympäristössä. Digitaalisessa ympäristössä rikollisten toimijoiden (ml. vakoilu) aiheuttaman pelon lisäksi on vältettävä käsitystä siitä, että viranomaiset seuraavat tai ”urkkivat” yksilöitä tai yrityksiä. ***Kielteisen kehityskulun torjumiseksi tulisi harkita, mitä ja miten tiedustelutoiminnasta sekä siihen liittyvän laillisuusvalvonnan tuloksista (ml. tuomioistuinkäytäntö sekä ministeriöiden lakimiesten toiminta) voisi tarjota tietoa elinkeinoelämän ja kansalaisyhteiskunnan käyttöön.***

Valtioneuvoston sisäisen turvallisuuden selonteko (VNS 4/2021 vp) korostaa tiedustelulla hankitun analysoidun tiedon merkitystä päätöksenteossa. Tämä on helposti hyväksyttävä tavoite. Mutta mitä päätöksiä tiedustelutiedon perusteella tehdään ja mitä katsotaan sisältyvän ”kansalliseen turvallisuuteen”? Asiasta on toki käyty kaukonäköistä keskustelua Eduskunnassa tiedustelulakien valmistelun yhteydessä. Vaikka elinkeinotoiminta tuottaa

Eteläranta 10, PL 10, 00131 Helsinki
www.fisc.fi

valtaosan yhteiskunnan aineellisesta hyvinvoinnista on epäselvää, huomioidaanko päätöksenteossa riittävästi elinkeinoelämän toimintaan liittyviä kysymyksiä. Erityisesti lainsäädännön kansantaloudellisten ja yritysvaikutusten seurantaan on siis kiinnitettävä edelleen huomiota. Myöskään **selonteko ei sisällä huomioita/arviota elinkeinoelämään kohdistuvista vaikutuksista.**

Empiirisen tiedon ja kokemuksen perusteella voidaan sanoa, että esimerkiksi terroristinen toiminta ei kykene perustuslaillisen oikeus- ja yhteiskuntajärjestyksemme murtamiseen eikä merkittävästi heikentämään yritysten kilpailukykyä tai toimintamahdollisuuksia. Lisäksi selonteostakin voidaan todeta, että Suomessa on ”yksittäisiä terrori-iskujen toteuttamisesta kiinnostuneita tahoja”. Näin asia on ollut hyvin pitkään. Elinkeinotoiminnan näkökulmasta vastatiedustelun ja vakoilun torjumista voitaneenkin pitää tärkeämpänä. Erityistä ***huomiota tulisikin kiinnittää tiedustelun avulla hankittujen tietojen luovuttamisen edellytyksiä rikostorjuntaan elinkeinorikoksia koskevissa tapauksissa. Samalla on tärkeää, että palomuurisääntelyn muutosharkinta ei johda poliisi- ja esitutkintalainsäädännön tarkoituksen kiertämiseen.***

Samalla on syytä huomioida, että niin luonnollisten henkilöiden kuin oikeushenkilöiden perusoikeussuojan (mm. aineettoman omaisuuden suoja ja viestinnän luottamuksellisuus) murentamisella voidaan heikentää merkittävästi taloudellista aktiivisuutta, toisin sanoen elinkeinotoimintaa, jonka fundamentti ovat luottamukselliset suhteet. Vertailukohdaksi sopinee vaikka Yhdysvallat, jonka ”rikos- ja turvallisuustiedustelun” laajuudesta ja sisällöstä kansalaisyhteiskunta ei pysty tekemään minkäänlaista selkoa. On siis oltava tarkkaavainen, että kun kansallista turvallisuutta uhkaavaa toimintaa torjutaan yhtäällä, jottei luottamusta nakerreta toisaalla. Tästä syystä ***myöskin rikostorjuntaviranomaisten oikeuksien laajentamiseen tulisi suhtautua hyvin varauksellisesti***.

Uusien teknologioiden aiheuttamien muutosten selvittämistä muiden palveluntarjoajien kuin teleyritysten teknologianeutraaliin avustamisvelvollisuuteen kansallisen turvallisuuden suojaamiskyvyn ja erityisesti kyberuhkien torjumisen kannalta voidaan pitää kannatettavana. Yrityksille asetettujen avustamis- ja tiedonluovutusvelvoitteiden vaikutuksia yritysten toimintaan on edelleen haastavaa arvioida. Niiltä osin viitataan lainsäädännön valmistelun aikana esitettyihin huomioihin yrityksille asetettujen velvoitteiden sekä niiden aiheuttamien kustannusten aiheuttamista vaikutuksista yritysten toimintaan. Lähtökohtaisesti yrityksille aiheutuvat **kustannukset tulee korvata** niille täysimääräisesti riippumatta siitä, aiheutuvatko ne teknisistä tai henkilökustannuksista. **Lisäksi kaikessa yritysyhteistyössä tulisi ottaa huomioon kansallinen ”kyberomavaraisuus”, mukaan lukien tietoverkkotiedustelun tai ns. offensiivisten kyvykkyyksien kehittämisessä.**

Kyberturvallisuusala on tällä hetkellä globaali kasvuala ja sillä on merkittävä kasvu- ja työllistämispotentiaali myös Suomessa. Kyberala korostaa, että tietoturvayrityksille tai muillekaan **ei tule asettaa vaatimuksia heikkouksien (esim. viranomaistakaporttien) tekemiseen tuotteisiinsa tai palveluihinsa.** Luotettavien tietoturvatuotteiden ja -palveluiden kannalta tällaiset velvoitteet romuttaisivat luottamuksen yritysten toimintaan ja tuotteisiin, jolloin niiden kilpailukyky markkinoilla katoaisi.

Lopuksi todettakoon, että elinkeinoelämän, sekä myös kansallisen kyberturvallisuuden edistämisen kannalta toivottavaa olisi, että tiedustelulainsäädännön selonteossa huomioitaisiin tiedustelun poikkeuksellisen syvälle perusoikeuksien alueelle ulottuvien vaikutustensa vuoksi nykyistä kattavampi arvio elinkeinoelämää koskevista oikeusvaikutuksista.

Eteläranta 10, PL 10, 00131 Helsinki
www.fisc.fi