VPO

22.1.2014

Muistio ei perustu nauhoitukseen, vaan tilaisuudesta tehtyihin muistiinpanoihin. Muistio ei välttämättä vastaa sanatarkasti käytyä keskustelua, mutta asiasisällön osalta käsityksemme mukaan vastaa tarkoitettua.

Liikenne- ja viestintäministeriön keskustelutilaisuus 21.1.2014 – Tiedustelun vaikutus sähköisen viestinnän luotettavuuteen

1. Yhteenveto

Lähes kaikki keskustelutilaisuudessa kuullut puheenvuorot korostivat sitä, kuinka tärkeää olisi käydä kyberturvallisuusstrategian toimeenpano-ohjelmassa ehdotetuista lainsäädäntöaloitteista erittäin laaja ja avoin yhteiskunnallinen keskustelu, jossa tulisi arvioida lainsäädäntömuutosten tarpeellisuutta verrattaessa niitä oikeusjärjestyksen nykytilaan ja sen mahdollisiin ongelmiin. Lisäksi keskustelussa tulisi pyrkiä erittäin huolellisesti arvioimaan sitä, millaisin eri vaihtoehdoin ongelmia voidaan ratkaista ja käytettävissä olevia vaihtoehtoisia keinoja tulisi punnita huolellisesti niiden erilaisten vaikutusten näkökulmasta.

Sähköisen viestinnän palveluita tarjoavien sekä niitä käyttävien yhteisöjen ja järjestöjen edustajien esittämien näkemysten mukaan luottamuksellisen viestinnän tiedusteluun ja tiedonhankintaan tähtäävät ehdotukset koetaan varsin ongelmallisiksi. Ongelmat ilmenevät perusoikeuksien toteutumisen, yritysten kilpailukyvyn, investointien houkuttelemisen, sekä yritysten asiakaslupausten näkökulmasta heikennyksinä nykytilaan. Samalla toimialan palveluntuottajien ja palveluiden käyttäjäyhteisöjen piirissä esitettiin voimakkaita epäilyjä myös siitä, onko toimenpideohjelman luonnoksessa ehdotettavilla tiedustelukeinoilla realistisia mahdollisuuksia saavuttaa niille asetettuja tavoitteita.

Viestintäpalvelujen tarjoajat ja niitä hyödyntävät elinkeinoelämän toimijat esittivät arvioita, joiden mukaan erittäin merkittävä ja kasvava osa liiketoiminnasta perustuu luottamukselliseen viestintään ja että tiedustelutoiminnalla saatettaisiin heikentää Suomessa yritysten kilpailukykyä, Suomen houkuttelevuutta investointien kohdemaana sekä yritysten kykyä ylläpitää asiakassuhteitaan ja täyttää asiakkailleen antamiaan lupauksia. Elinkeinoelämän edustajien esittämien arvioiden mukaan viestinnän luottamuksellisuutta rajoittava tiedustelu saattaisi vahingoittaa Suomen mainetta ja lisätä liiketoiminnan Suomeen sijoittautumisessa huomioitavaa niin sanottua maariskiä.

Erilaisia nykylain sallimia teknisiä ja hallinnollisia toimenpiteitä (esimerkiksi teknisten salaustuotteiden käyttö ja muut ns. tietoturvatoimenpiteet) esitettiin ratkaisuina, joilla voitaisiin huolehtia tietoturvallisuudesta ja suojautua laittomalta vakoilulta eri yhteisöissä. Luottamuksellista sähköistä viestintää tarjoavien tai esim. salaustuotteita valmistavien yritysten velvoittaminen tiedustelua tarkoittaviin toimiin olisi erittäin haitallista näille yrityksille, joista osa voisi omien arvioidensa mukaan joutua harkitsemaan tarvetta siirtää toimintojaan velvoitteiden vuoksi pois Suomesta. Lisäksi teleyrityksien edustajat korostivat, että jo nykylakien suomilla viranomaisvaltuuksilla poliisiviranomaisilla on mahdollisuudet hankkia varsin kattavasti tietoja kybertoimintaympäristöön liittyvistä rikoksista.

Sähköisen viestinnän palveluntarjoajia edustavat yritykset totesivat että, huomattava osa kansalliseksi mielletystä viestiliikenteestä kulkee myös Suomen rajojen ja lainkäyttöpiirin ulkopuolella. Tämä tarkoittaa palveluntarjoajien mukaan sitä, ettei signaalitiedustelua olisi edes teknisesti tosiasiassa mahdollista kohdistaa siten, että Suomen kansalaiset jäisivät tiedustelun ulkopuolelle, vaan rikosepäilyihin kytkeytymätön valvonta koskettaisi kaikkia suomalaisia - myös esimerkiksi eduskuntaa ja ministeriöitä. Asia nousi esiin varsin periaatteellisena kysymyksenä ja oikeushyvien kollisiotilanteena. Toimivaltuuksien tosiasiallisesti toimivan valvonnan ja oikeussuojakeinojen järjestämiseen nähtiin varsin hankalana.

Liikenne- ja viestintäministeriö
Käyntiosoite: Eteläesplanadi 16 (kirjaamo) 00100 Helsinki
Postiosoite: PL 31 00023 Valtioneuvosto
Puhelin: 029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

Yliopistojen ja ns. kasvuyritysten edustajat toivat esiin sen, että verkkotiedustelu on kansantaloudellisesti merkittävä kysymys ja he toivoivat asian huomioimista jo valmistelun varhaisessa alkuvaiheessa. Suomella voisi useiden tilaisuudessa edustettujen tahojen mukaan olla suuria taloudellisia mahdollisuuksia pilviteknologian kehittämisessä ja rakentamisessa. Suomella on hyvät mahdollisuudet lisätä entisestään tänne suuntautuvia pilviteknologian investointeja. Tietoturvasta ja yksityisyyden suojan kunnioittamisesta tulisikin useiden eri toimialoja edustavien yritysten, yhteisöjen ja kansalaisjärjestöjen arvion mukaan tehdä Suomelle vientituote. Muiden valtioiden ylimitoitettujen vakoilutoimien vuoksi Suomella olisi niiden mukaan mahdollisuuksia profiloitua korkean tietoturvan maana, jonne haluaisivat sijoittautua ja investoida kenties sellaiset yritykset, jotka aikovat sitoutua korkeaan tietosuojan tasoon.

Tiedustelun ongelmana mainittiin myös liikesalaisuuksien vuotaminen sellaisiin käsiin, jotka eivät tietoihin ole oikeutettuja, mikä voisi olla vahingollista Suomessa toimivien yritysten kilpailukyvyn ja ulkomaisten yritysten investointihalujen kannalta. Keskustelutilaisuudessa kuullun perusteella tietoturvan parantamiseksi olisikin oletettavasti tehtävissä paljon tehokkaampia ja tarkoituksenmukaisempia toimenpiteitä kuin luottamuksellisen viestinnän tiedustelun aloittaminen. Tiedustelun mahdollista vaikuttavuutta kyberuhkien torjumiseen pidettiin lopulta varsin heikkona.

2. Seminaariavaus – asunto- ja viestintäministeri Pia Viitanen

Ministeri Viitanen toivotti vieraat tervetulleiksi tilaisuuteen ja kiitti alustuspuheenvuorojen pitäjiä. Puheessaan ministeri painotti viestinnän luottamuksellisuuden merkitystä jokaisen ihmisen elämässä. Viimeaikoina esiin tullet paljastukset, ovat avanneet aivan uuden maailman, jossa tiedustelussa on menty pidemmälle kuin mitä on pidettävä hyväksyttävänä. Ministerin mukaan asiaan pitäisi saada yhteisiä kansainvälisiä pelisääntöjä ja siitä tulisi käydä avointa keskustelua.

Ministeri nosti myös esiin maailmassa käynnissä olevan digitaalisen kehityksen. Viisas Suomi ymmärtää hyödyntää kaiken sen potentiaalin, jota internetillä on. Vaikka Suomessa on jo tehty paljon asioita, kuten päätökset uusista merikaapeleista ja sähköverotuksen tarkastamisesta, niin silti on vielä paljon asioita, joita tulevaisuudessa tulisi tehdä.

Lopuksi ministeri totesi, että Suomessa on totuttu siihen, etteivät ulkopuoliset pääse lukemaan sähköpostiviestintää tai mitään muutakaan viestintää. Tiedustelua harkittaessa tulee kiinnittää huomiota siihen, että keino suhteessa tavoitteeseen on avoin ja kestävä.

3. Ehdotuksen vaikutukset tietoturvaviranomaisen näkökulmasta – Asta Sihvonen-Punkka, Viestintävirasto

Sihvonen-Punkka esitteli puheenvuorossaan, mitä Viestintävirasto on tehnyt Snowden paljastusten jälkeen ja miten virasto näkee aihepiirin jatkotarkastelun. Sihvonen-Punkka kertoi kybertuvallisuuskeskuksen perustamisesta ja viestintäviraston tehtävistä yleisemmin. Hän kertoi myös, miten Viestintävirasto on selvittänyt Snowden-paljastusten mukaisen urkinnan vaikutuksia suomalaisiin viestintäpalveluiden käyttäjiin. Selvitystä tehtiin lähettämällä teleoperaattoreille, näiden käyttämille ulkomaisille alihankkijoille sekä laitevalmistajille selvityspyyntöjä. Selvityksessä havaittiin, että teleyritykset voivat suojata tiedot omissa palveluissaan, mutta viestinnän luottamuksellisuuden turvaaminen ostettaessa palveluita alihankintana Suomen ulkopuolelta voi olla hankalaa. Jatkotoimenpiteinä nimettiin viranomaistiedotuksen lisääminen ja teleyritysten ulkomailla tuotettujen palveluiden turvallista toteuttamista varten on perustettu työryhmä.

Lopuksi Sihvonen-Punkka esitteli Viestintäviraston näkemystä siihen, miten tiedusteluun liittyvää lainsäädäntöä tulisi arvioida. Ensiksi tulisi suorittaa perusteellinen vaikutusarviointi. Siinä selvitettäisiin puolin ja toisin ongelmia, eli sitä minkälaisia tarpeita viranomaisilla olisi ja mitä vaikutuksia toimilla voisi olla esim. investointihalukkuuteen. Myös toiminnan tavoitteet tulisi perusteellisesti hahmottaa. Tämän jälkeen keinot tavoitteiden saavuttamiseen tulisi koota yhteen ja niitä tulisi vertailla keskenään. Vasta tämän jälkeen voitaisiin tehdä ehdotus valittavasta keinosta. Tällaisella prosessilla voitaisiin saada aikaan paras mahdollinen lopputulos. Johtopäätöksenä Sihvonen-Punkka totesi, että tiedusteluun liittyvää lainsäädäntöä on valmisteltava avoimesti ja siinä on arvioitava yksityisyyden suoja huomioiden kyberturvallisuuden tarpeita.

4. Ehdotusten vaikutukset perusoikeuksien näkökulmasta – Tuomas Ojanen, Helsingin yliopisto

Ojanen aloitti puheenvuoronsa toteamalla, että tyhjästä on paha nyhjästä. Lausunnolla olevassa kyberturvallisuusstrategian toimeenpano-ohjelmassa ei nimittäin puhuta ollenkaan perus- tai ihmisoikeuksien toteutumisesta. Lainsäädäntöhankkeessa perus- ja ihmisoikeusnäkökulma on otettava jo alusta asti huomioon prosessissa. Puheenvuorossa esitettiin kaksi keskeistä kysymystä tiedustelutoiminnan tarkastelemiseen perus- ja ihmisoikeusnäkökulmasta. Ensimmäinen kysymys liittyy siihen, rajoitetaanko toiminnalla perus- ja ihmisoikeuksia ja toinen siihen, täyttyvätkö perusoikeuksien rajoitusedellytykset.

Tiedustelutoiminnan ollessa kyseessä lienee selvää, että useampiakin perus- ja ihmisoikeuksia rajoitetaan kuin vain yksityisyyden suojaa. Muina perusoikeuksina mainittiin yhdenvertaisuus, syrjimättömyys, sananvapaus sekä yleisemmin ihmisten mahdollisuus osallistua internetmaailmaan. Tiedustelua ei voida suunnata vain tiettyihin ihmisryhmiin esimerkiksi etnisen alkuperän perusteella.

Perusoikeuden rajoitukselle tulee olla peruste laissa, perusteen tulee olla hyväksyttävä, rajoituksen tulee myös olla täsmällinen ja tarkkarajainen ja sen tulee olla välttämätön ja oikeasuhtainen. Perus- ja ihmisoikeuksia ja niiden rajoittamista arvioitaessa tulee myös huomioida, että nämä oikeudet koostuvat ydin- ja reuna-alueista. Esimerkiksi luottamuksellisen viestinnän suojassa ydinaluetta on viestinnän sisältö, jonka rajoittamiseen suhtaudutaan tiukemmin, kun taas pelkkiin tunnistetietoihin on suhtauduttu hieman väljemmin.

Lisäksi korostettiin sitä, ettei perus- ja ihmisoikeusarviointia voida suorittaa jälkikäteen ja liimata lainsäädäntöprosessiin päälle. Tällaiset hankkeet tulee järjestää niin, että niissä harkitaan jo etukäteen lainsäädännön perus- ja ihmisoikeusulottuvuuksia

5. Ehdotusten vaikutukset sähköisen viestinnän palveluita käyttävien kansalaisten näkökulmasta – Ville Oksanen, Effi ry

Tiedustelua koskevan lainsäädännön valmistelussa on tällä hetkellä vain virkamiehiä mukana, eikä edes tietosuojavaltuutetun toimistosta ketään. Uudenlaisen turvallisuuden maailmassa myös kansalaiset ja yhteiskunta ovat kuitenkin keskeinen osa turvallisuutta. Oksanen totesi kuitenkin, että on mahdollista laatia lainsäädäntöä vakavan rikollisuuden torjumiseksi välttämättömästä tiedonhankinnasta. Tämän tulisi vain olla tarpeeksi läpinäkyvää ja mahdollistaa esimerkiksi sen kertomisen kuka pyytää, mitä ja keneltä. Oksanen viittasi myös Ojasen puheenvuoroon tunnistetietojen keräämisestä ja totesi, että ihmisiä pystytään jo nyt tehokkaasti profiloimaan pelkillä tunnistetiedoilla, joten niitäkin tulisi siis suojata kuten viestien sisältöä.

Oksasen mukaan Suomella on nyt Snowden-tapauksen jälkeen kaksi mahdollista tietä: tietosuojan Sveitsi tai FRA-kateus. Puheenvuorossa esitettiin perusteluja sille, miksi Suomi voisi olla globaalisti hyvän tietojen tallentamispaikka. Suomi ei

kuulu NATO:on ja on yllättävän lähellä Aasiaa. Suomessa on myös kylmä ilmasto ja vähän korruptiota suhteessa muihin maihin. Aktiivinen tietosuojan valvonta, jota tarvitaan, on hankalaa erityisesti nykyisillä resursseilla.

Oksanen totesi, ettei kysymys ole siitä, että Suomeen tulisi luoda jonkinlainen internetin villi länsi. Pikemminkin Suomeen tulisi luoda sellainen ympäristö, jonne sijoittuu yrityksiä, jotka haluavat sitoutua korkeaan tietosuojaan. Tämä tarkoittaisi myös tiukkaa regulaatiota, jolla houkuteltaisiin toimijoita.

6. Ehdotusten vaikutukset sähköisen viestinnän palveluntarjoajan näkökulmasta – Jukka Leinonen, DNA

Leinonen totesi, että on haasteellista, ettei mahdollista tiedusteluun liittyvää lainsäädäntöä ole valmisteltu kovinkaan avoimesti. Mukana ei ole ollut yrityksiä, vaikka olisi tärkeä, että erilaiset näkökannat otetaan huomioon. Kattavan analyysin jälkeen on helpompi tehdä oikeita valintoja ja vähentää myös haittavaikutuksia.

Liiketoiminnallisesta näkökulmasta todettiin, että kaikki mikä voidaan digitalisoida, tullaan digitalisoimaan. Kilpailukyvyn kannalta ja investointikohteena Suomella voi olla hyvät edellytykset saada tänne globaalejakin digitaalisen maailman palveluntarjoajia. Asiakkaiden tulee myös voida luottaa palveluihin ja nähdä selkeät pelisäännöt niitä käyttäessään. Jos tietoja luovutetaan eteenpäin, tulee asiakkaan tietää ja ymmärtää tämä. Elinkeinoelämän ja kilpailukyvyn näkökulmasta voidaan katsoa, että tiedustelutoiminnalla menetettäisiin tiettyjä kilpailukykyyn liittyviä elementtejä.

Jos päädytään taloudellisesti raskaaseen ratkaisuun, niin taloudelliset panostukset tulee korvata niille yrityksille, jotka toimintaa ylläpitävät. Lisäksi kyberturvallisuuskeskus tulisi huomioida valmistelussa, jotta viranomaisorganisaatiot täydentäisivät toisiaan, mutta eivät olisi päällekkäisiä.

Leinonen kannatti Sihvonen-Punkan esittelemää prosessitapaa lainsäädännön valmisteluun ja totesi, että kyberturvallisuusstrategian päätavoitteet ovat hyvät, mutta valmistelun tulee olla avointa ja monitahoista, jotta löydetään paras tapa toteuttaa tavoitteet.

7. Ehdotusten vaikutukset sähköisen viestinnän palveluita käyttävien yritysten näkökulmasta – Jyrki Hollmén, EK

Hollmén totesi, ettei ota kantaa siihen, tarvitaanko Suomeen tiedustelutoimintaa ja sitä koskevaa lainsäädäntöä. Kansainvälinen toimintaympäristö kehittyy koko ajan ja tilannekuvan, siitä mitä verkoissa tapahtuu ja onko yhteiskunnalla mahdollisuus suojautua, tulee olla oikea. FRA:ssa tietoa on kerätty tiettyä käyttötarkoitusta varten, mutta on muistettava, että tiedosta tulee helposti kauppatavaraa. Ajaudumme helposti tilanteeseen, jossa on käynnissä valtioiden kilpavarustelu ja aina kun USA tekee jotain niin muut menevät perässä. Hollmén totesi myös, että tietojenkäsittelyä tulisi opiskella jo alakoulusta lähtien ja että siviilielämään kohdistuvat taloudelliseen hyötyyn perustuvat kyberrikokset ovat kasvussa.

Hollménin mukaan Suomessa tulee tiedostaa, että elämämme viennistä ja myös tiedustelutoimintaa tulee arvioida tästä lähtökohdasta. Toisaalta viranomaisilla tulee olla riittävät toimivaltuudet, mutta toisaalta niiden optimaalisuutta suhteessa elinkeinoelämään tulee punnita. Panos/tuotos -suhdetta tiedustelutoiminnassa voi olla vaikeaa arvioida, koska viranomainen saa tuotoksen, mutta yksityinen ylläpitää toimintaa.

Tiedustelu voi Hollménin mukaan aiheuttaa yritysten asiakas-suhteisiin ja lupauksiin sellaisen särön, jota on hankala täyttää. Jos yrityksen liiketoiminta perus-

tuu luottamukselliseen viestintään, niin tiedustelutoiminnan aloittaminen vaikuttaa tietysti tällaiseen toimintaan. Pilvipalveluiden investointien ollessa 200 miljardia vuodessa tämä näkökulma on merkittävä. On myös esitetty arvioita siitä, että amerikkalaiset pilvipalveluiden tarjoajat voivat menettää tiedustelukohun seurauksena seuraavan kolmen vuoden aikana pahimmillaan jopa 20 prosenttia Yhdysvaltain ulkopuolisesta liikevaihdostaan. Hollménin mukaan tiedustelutoiminta voisi luoda Suomelle brändiriskin, koska meillä on hyvä maine maailmalla. Lisäksi myös maariski sekä mahdolliset kaupan esteet ja vastareaktiot olisi huomioitava.

Lainsäädännön valmisteluprosessista Hollmén esitti kysymyksen, olisiko hyödyllisempää tai oikeellisempaa pohtia laajapohjaisessa työryhmässä laajemmin tiedustelulainsäädäntöä. Kyseessä on asia, joka koskee koko kansakuntaa. Lainsäädäntötyössä tulisi arvioida, mitä uhkia halutaan torjua ja käydä myös läpi suomalaisen tiedustelun nykytilannetta. Toimeenpanoehdotuksissa tulisi myös käyttää hyväkseen yksityistä sektoria. Tällä hetkellä toimijat eivät ole lähelläkään lainsäädäntötyötä.

8. Ehdotusten vaikutukset EU:n kilpailuasemaan luotettavien digitaalisten sisämarkkinoiden kehityksessä – Mika Lauhde, SSH Secure Communications Oyj

Lauhde aloitti puheenvuoronsa toteamalla, että yleensä kun signaalitiedustelu alkaa, niin sen jälkeen keskustelua ei enää käydä julkisesti, ennen kuin tulee joku, joka kertoo miten pitkälle toiminnassa on menty alkuperäisestä mandaatista. Vakoilua ei myöskään pystytä reguloimaan, koska sääntelyä ei pystytä valvomaan. Tämän vuoksi Suomessa voitaisiin keskittyä tietoturvan parantamiseen tietoliikenteen salaamisella ja muilla tietoturvatoimenpiteillä. Salausten tekeminen on aina helpompaa kuin niiden avaaminen.

Snowden-skandaalin merkit olivat nähtävissä jo kauan aikaa sitten, ainoastaan tiedustelun laajuus yllätti. EU on elänyt jo pidempään kaiken kieltämisen aikakautta, mutta ns. Belcacom -tapauksesta sen on vaikea toipua. Kansallisten järjestelyjen aikakausi on ohi. Koko Euroopan laajuista tietoturvaa on jo pyritty rakentamaan, mutta johtavat EU-jäsenvaltiot ovat nähneet sen uhkana kilpailukyvylleen. Jos tilannetta katsotaan globaalista näkökulmasta, niin on kyse taloudellisesta hyvinvoinnista, eli siitä että omalle maalle saadaan isompi pala kakusta kuin muille. Laude puhui myös Ruotsin FRA:n signaalitiedustelusta. Se on ollut, hyvä järjestely Ruotsille, jonka menestys on johtunut mm. siitä, ettei Suomi salaa tietoliikennettään.

Jos tiedustelutoiminta mahdollistetaan voi suomalaisten yritysten luotettavuus kärsiä ja voi herätä myös epäilyksiä yritysten pakottamisesta viranomaisyhteistyöhön. Koska tietoturva on luottamusbisnestä joutuvat yritykset harkitsemaan Suomesta lähtemistä, jos herää epäilyjä takaporttien asentamisesta tms. Yritykset siirtyisivät tällöin maihin, joissa ei tiedustelutoimintaa ole tai maihin, joissa on, mutta niitten sisäiset markkinat ovat niin suuret, että se kompensoi tiedustelun taloudelliset haitat.

Keskeinen kysymys on, minkälainen brändi ja liiketoimintaympäristö Suomeen halutaan luoda. Konesalit ovat kriittistä infrastruktuuria yrityksille ja myös niille maille, joista konesaliyritykset tulevat. Ne myös tuottavat paljon salattua tietoa, jota on vaikeaa käyttää hyväksi. Mitä enemmän salattua tietoa verkoissa liikkuu, sitä vaikeampi on löytää mielekästä tietoa tiedustelulla. Esimerkiksi SSH:n salauksia ei ole enää avattavissa sellaisilla tietokoneilla, joita Suomen resursseilla voitaisiin tiedustelutoimintaan hankkia.

Suomi voi halutessaan olla joko mini-NSA tai tietosuojan Sveitsi. Uskottavaan NSA:han Suomella ei resurssien puolesta ole mahdollisuutta. Lauhteen mukaan on selvää, että tietoa kerätään kaupankäyntiin, mutta sellaiseen, josta ei jää kir-

janpitoon jälkiä. Tämänkin takia tietoliikenteen salaaminen olisi edullinen vaihtoehto ja siitä olisi myös kansantaloudellista hyötyä.

9. Keskustelu

Ministeriöiden ja muiden viranomaisten edustajat

Tietosuojavaltuutetun toimiston edustaja

Todettiin, että kyberturvallisuusstrategiassa ja sen toimeenpano-ohjelmaluonnoksessa on loistavia asioita ja hyviä avauksia. Siinä korostetaan osaamista ja kilpailukykyä, sekä sillä pyritään varautumaan identiteettivarkauksiin. Osa näistä on toisaalta kuitenkin n. 15 vuotta myöhässä.

Kannatettiin ”Security Valley” -idean omaksumista ajatustasolla Suomeen. Tämä voisi edistää suomalaista kilpailukykyä. Pidettiin myös tärkeänä käydä päätöksentekijöiden, eli poliitikkojen ja turvallisuusviranomaisten välistä keskustelua tiedustelusta. Koska tiedustelussa on kyse perus- ja ihmisoikeuksiin puuttumisesta, tarvitaan asiasta lainsäädäntöä. Eduskuntaan tulee myös antaa riittävästi tietoa aiheesta, jotta se aikanaan osaa tehdä oikeat päätökset. Päättäjien kokonaiskuva asioista on usein sirpaleinen, kun lainsäädäntöä uudistetaan pieni pala kerrallaan.

Huomautettiin, että Suomessa on usein tapana alkaa toimia vasta kun maito on jo maassa. Kun nousee esiin jokin skandaali, niin heti mietitään, pitäisikö lakeja muuttaa ennen kuin edes arvioidaan nykytilaa, jonka tarkemmassa tarkastelussa saatetaankin huomata, että asia olisi ollut ratkaistavissa jo olemassa olevilla keinoilla ja että niitä ei ole käytetty tai osattu käyttää tapauksessa.

Tiedustelussa ei ole kyse kyllä tai ei asetelmasta, vaan asiasta tarvitaan tietoa. Iso asia tulee pilkkoa pienempiin kokonaisuuksiin ja tätä kautta miettiä ratkaisuja. Yksityisyyden osalta lainsäädännön tulee ilmentää oletusarvoista tietosuojaa (”privacy by design”). Samoin tulee pohtia tietojen käyttötarkoitusta. Jotta tiedustelua voitaisiin toteuttaa järjestelmällisesti, tulisi sen valvonta järjestää hyvin. Katsottiin myös, etteivät olemassa olevat viranomaiset (TSV /Viestintävirasto) välttämättä soveltuisi valvojiksi ja korostettiin, että tämä on tärkeä osa-alue pohdittavaksi.

Lisäksi nostettiin esiin kansalaisnäkökulma. Englantilaiset kollegat olivat käyneet läpi ITunesin käyttäjäehdot ja todenneet niiden sisältävän 90 000 sanaa, siis enemmän sanoja kuin Shakespearen Hamletissa. EU:ssa valmistelussa oleva tietosuoja-asetus olisi siirtämässä palveluntarjoajille vastuuta asiakkaiden tietosuojasta. Tietosuojan toteutuminen vaatii kuitenkin myös valvontaa. Lisäksi todettiin, että YK:ssa on tehty globaali aloite siitä, että kansalaisten oikeuksia koskevaan sopimukseen otettaisiin osaksi myös kansalaisten digitaaliset oikeudet.

Puolustusministeriön edustaja

Todettiin, että luonnos kyberturvallisuusstrategian toimeenpano-ohjelmasta, joka osallistujille on lähetetty ja lainsäädäntö ryhmä, joka pohtii vain yhtä osaa toimeenpano-ohjelmasta, tulisi pitää erillään toisistaan.

Todettiin, että lainsäädäntötyötä ei ole tarkoituksena pitää pienen piirin tiedossa. Ajatuksena on nimenomaan ollut, että kun on kartoitettu, mitä hallinnonalat ovat mieltä asiasta ja on saatu jotain konkreettista kommentoitavaksi, niin sitten kuullaan, kentän mielipiteitä ja käytetään tätä tietoa jatkovalmisteluissa. Ensin tulee pohtia, mihin uhkiin tulisi edes vastata lainsäädännöllä. Arvioinnissa kuullaan turvallisuusviranomaisia, kartoitetaan nykytilaa ja kehittämistarpeita, jonka jälkeen haarukoidaan lainsäädännöllisiä mahdollisuuksia.

Tuotiin esiin hallituksen linjaus ryhtyä asiassa välittömästi toimeen, mutta painotettiin, että koko Suomen osaaminen tulee hyödyntää lainsäädäntötyössä. Työ tulee etenemään kuten aivan normaali lainsäädäntöprosessi, eli ensin tehdään työryhmän mietintö, tämän jälkeen mahdollinen HE ja sitten asiasta keskustellaan asianmukaisesti eduskunnassa. Työryhmä on kokoontunut vain kaksi kertaa, joten tämä on syynä siihen, miksi asiasta ei ole vielä kuultu.

Keskustelussa tulisi olla varma siitä, että tiedustelu ymmärretään samalla tavalla. Tulee erottaa se mikä on tiedustelua, mikä rikosten ennaltaestämistä ja mikä pakkokeinojen käyttöä.

Viestikoelaitoksen edustaja

Todettiin, että jaetaan kaikki huolet, joita tilaisuudessa on esitetty, vaikka näkökulma aiheeseen onkin toinen. Viestikoelaitos haluaa nimenomaan turvata suomalaista kilpailukykyä, mutta jakaa myös huolet esimerkiksi perusoikeuksiin puuttumisesta. Tiedustelu liittyy puolustus- ja turvallisuustoimintaan esimerkiksi sotilaallisten uhkien, Suomea koskettavien kansainvälisten kriisien sekä vieraiden valtojen tiedustelutoiminnan havaitsemiseen. Teollisuusvakoilu ei kuulu Suomen sotilastiedustelun tehtäviin. Tarkoituksena tiedustelulla ei ole mitenkään heikentää sananvapautta tai esimerkiksi lehdistön lähdesuojaa.

Turvallisuusviranomaiset eivät ole Suomessa julkaisseet kyberturvallisuudesta uhka-arvioita, mutta yksi esimerkki toteutuneesta uhkasta oli UM-tapaus. Kerrottiin myös, että Norjassa havaittiin 50 vakavaa kybervakoilutapausta vuonna 2012.

FRA:n julkisuuteen antaman tiedon mukaan Ruotsiin kohdistuva ulkovaltojen tiedustelutoiminta kohdistuu valtion organisaatioihin, tutkimuslaitoksiin, yliopistoihin ja yrityksiin ja horjuttaa Ruotsin kilpailukykyä kansakuntana. Jos Suomessa havainnointikyky ei olisi puutteellinen, koko tiedustelua ei esitettäisi. Tulevan lain tulisi myös olla sellainen, että se mahdollistaa myös yritysten suojaamisen. Lisäksi todettiin, että ajatus palveluiden turvasataman perustamisesta on kannatettava asia, mutta asiaa voi miettiä siltä kannalta, että kannattaisiko Suomesta luoda ilmailun turvasatama lopettamalla ilmavalvonta

Lopuksi todettiin vielä, että jaetaan vahvasti Tuomas Ojasen näkökulma ja että kansalaisten ja yritysten tiedoilla ei ole tarvetta käydä kauppaa. Tiedustelun tarkoitus on turvata perusoikeudet Suomessa myös jatkossa.

Poliisihallituksen edustaja

Todettiin, että poliisi on toimija, joka on pitänyt pesänsä puhtaana ja mm. tutkinut teleoperaattoreiden tietojen jakamisessa tekemiä ylilyöntejä. Lisäksi huomautettiin, että kaikki keskustelijat lähestyvät luonnollisesti eri näkökulmista aihetta ja omista premisseistään käsin.

Puolustusvoimien realiteetit ovat muuttuneet ja yhä enemmän rikoksia tehdään tietoverkoissa. Poliisin osalta pitää löytää uusia lähestymistapoja tietoverkkorikollisuuteen. Myös oikeudellinen sääntely voi olla tässä suhteessa ongelmallista, koska reaalimaailman sääntely ei välttämättään logiikaltaan vastaan sääntelyä, jota tarvittaisiin tietoverkkoihin. Tulisi myös yleisesti pohtia, pätevätkö samat periaatteet enää reaalimaailmassa kuin tietoverkossa.

Suojelupoliisin edustaja

Todettiin, että tilaisuudessa on ollut hyvää keskustelua. Kaikki me olemme samassa veneessä. Kyseessä on turvallisuus, niin kansalaisten kuin yritystenkin. Vastakkain asettelua tiedusteluviranomaisten ja kansalaisten välillä on tarpeetonta korostaa. Tasapaino eri näkökulmien välillä on löydettävissä ja keskeistä

onkin määritellä riittävän tehokkaat keinot ja niiden valvonta. Suomalaisten intressien suojeleminen maailmalla on tärkeää.

Teleoperaattoreiden edustajat

Operaattoreiden edustajat yhtyivät Sihvonen-Punkan ajatukseen aiheen syvällisestä analysoinnista ja valmistelun avoimuudesta. Valmistelussa tulisi myös käydä läpi olemassa olevat pakkokeinot, joita voitaisiin käyttää ja se tarvitaanko ylipäätään uutta sääntelyä. Lisäksi todettiin, ettei hankkeelle tulisi asettaa epärealistisia odotuksia.

Operaattorit toivat myös esille teknisen näkökulman hyödyntämistä lainsäädäntöprosessin aikana ja peräänkuuluttivat tietoverkkojen toiminnan ymmärrystä. Huomattava osa liikenteestä, joka mielletään kansalliseksi, kulkee todellisuudessa Venäjän tai Ruotsin kautta, eikä pysy Suomen rajojen sisällä. Tämä tarkoittaa sitä, että tiedustelulla alettaisiin kuunnella kaikkia suomalaisia myös esimerkiksi eduskuntaa ja ministeriöitä. Kyse on periaatteellisesta kysymyksestä, jossa oikeushyvät ovat kollisiotilanteessa. Myös tiedustelutoiminnan valvonnan järjestämiseen nähtiin hankalana.

Yliopistojen edustajat

Yliopistojen edustajat toivat esiin tiedustelun olevan kansantaloudellisesti merkittävä kysymys ja toivoivat tämän huomioimista jo valmistelun alkuvaiheessa. Suomella voisi olla suuria taloudellisia mahdollisuuksia pilviteknologian kehittämisessä ja rakentamisessa. Tämä vaatisi myös laajempaa viranomaisten sekä akateemisen ja yritys-maailman yhteistyötä. Seuraava vuosikymmen tulee olemaan yritysten sijoittautumispäätösten kannalta kriittinen aikakausi ja ne maat, jotka saavat datateollisuutta sijoittumaan alueelleen tulevat hyötymään siitä taloudellisesti.

Tiedustelun yhdeksi ongelmaksi nostettiin liikesalaisuuksien vuotaminen sellaisiin käsiin, jotka eivät niihin ole oikeutettuja. Myös internetin globaaliluonne nostettiin esiin. Vaikka Suomessa tehtäisiin kuinka hyviä säännöksiä, niiden valvominen muualla on mahdotonta.

Puheenvuoroissa todettiin, että erityisesti yhteiskunnan toiminnan kriittistä infrastruktuuria sisältäviä ja valtiollisia verkkoja tulisi suojella paremmin. Tietoturvan parantamisen kannalta olisi tehtävissä paljon muutakin kuin tiedustelun aloittaminen. Voitaisiin esimerkiksi rahalla tai jollain muulla keinolla pakottaa toimijoita tekemään yhteistyötä tietoturvan parantamiseksi. Lisäksi kyseenalaistettiin tiedustelun vaikuttavuutta kyberuhkien torjumiseen, kun esimerkiksi hyökkäyksien jälkiä voidaan helposti peittää. Myös ilmapiiri, jossa tietovuodoista ei uskalleta maineen menettämisen pelossa kertoa julkisesti, nähtiin ongelmallisena.

Ohjelmisto- ja datakeskusliiketoiminnan edustajat

Ohjelmisto- ja datakeskusliiketoiminnan edustajat yhtyivät laajasti esitettyihin alustuksiin. Toimijat toivoivat avointa valmistelua ja mahdollisuutta päästä esittämään omia näkökantoja lainsäädännön valmistelussa. Toisaalta kiiteltiin myös lainsäädäntöprosessille annettua lyhyttä määräaikaa, koska usein viranomaisten valmistelu on monimutkaista ja kestää pitkään.

Tiedustelutoimintaa harkittaessa tulisi huomioida Suomen mahdollisuus luoda merkittävää kilpailuetua ajamalla ”data Sveitsi” ajatusta eteenpäin. Myös jo harkinnassa olevat investoinnit esimerkiksi datakeskusliiketoimintaan tulisi ottaa huomioon. Tietoturvalla voitaisiin myös saada Suomelle uusi vientituote ja sen kautta sillä voitaisiin luoda lisää työpaikkoja.

Tietoturvan eteen on jo tällä hetkellä tehtävissä paljon ja ei tulisi unohtaa, että jokaisen organisaation on jo nyt mahdollista hoitaa tietoturvaansa hyvin. Urkintaa ei voikaan perustella pelkästään tietoturvalla. Myös virka-avun laajentamista ja suosimista toivottiin sekä nostettiin esiin myös public / private -yhteistyön lisääminen.

Tiedustelutoiminnan toivottaisiin olevan tarkkaan rajattua, molempiin suuntiin läpinäkyvää ja se tulisi kohdistaa vain tiettyihin ihmisiin. Lisäksi huomiota tulisi kiinnittää myös tietojen suojaamisen kehittämiseen.