



28.1.2010

Valtiontalouden tarkastusviraston pääjohtaja, dosentti, OTT Tuomas Pöystin puheenvuoro valtiontalouden tarkastusviraston ja tietosuojavaltuutetun IT –foorumissa 28.1.2010

KILPAILUKYKYINEN SUOMI TARVITSEE SELKEÄN TIETOTURVALLISUUSLAIN

Tietoturvallisuus on huomattavan oikeudellistunut mutta mistä näkökulmasta tietoturvallisuuslakia olisi pohdittava?

Tiedonhallinnan mallit ja tietotekniikka määrittävät organisaatiotavat ja vaikuttavat oikeuteen

Tietoturvallisuuden ja lain suhde on kertomus siitä, kuinka käytettävissä olevat ja valitsevat teknologiat vaikuttavat oikeuteen sekä organisaatioiden muotoon ja toimintatapaan. Organisaatioiden muoto ja toimintatapa vaikuttavat puolestaan oikeudellisiin sääntelytarpeisiin ja oikeuden sisältöön jo siitä yksinkertaisesta syystä, että oikeuden perustehtäviä on sosiaalinen koordinaatio. Oikeuden tehtäviä on myös antaa hallinnan ja toiminnan välineitä taloudelliseen toimintaan ja muuta ihmisten yhteistyötä ja yhteiselämää varten. Tieto- ja viestintätekniikan ja niiden hyväksikäytön muuttuessa muuttuvat myös sosiaalisen koordinaation ja hallintavälineiden tarpeet. Taloustieteellisestä näkökulmasta yhden professori Matti Pohjolan ajatukseen siitä, että *tieto- ja viestintätekniikan hyödyntämisen vallankumous on vasta alkanut*.

Olin 12 vuotta sitten mukana kirjoittamassa valtiovarainministeriön toimeksiannosta Lapin yliopistossa tehtyä Tietoturvallisuus ja laki –tutkimusta. Sen yhtenä suositukseksi oli yleisen tietoturvallisuuslain säätäminen Suomeen. Näkökulmaa pidettiin tutkimusraportin tilaajia ja tilaaman edustajia – joista haluan mainita erityisesti hallitusneuvos Miliza Vasiljeffin ja tuolloinen VM:n neuvotteleva virkamies Kaarlo Korvolan – lukuunottamatta outona. Tietoturvallisuus näkyi Suomen oikeudessa hajanaisina säännöksiä ja erityisesti eduskunnan oikeusasiamiehen ja korkeimman oikeuden tietoturvallisuudesta huolehtimisen velvoitteen yleisiin oikeusperiaatteisiin, kuten hallinnon lainalaisuusperiaatteeseen, toimeksiannon saajan yleisiin sopimusoikeudellisiin velvollisuuksiin ja sopimuslojaliteettiin liittäminä periaatteina. Tietoturvallisuus oli toki ajatuksellisesti sisällä vanhassa henkilörekisterilaissa (471/1987). EU:n henkilötietodirektiivin myötä tietoturvallisuudesta tuli nimenomaiset, mutta direktiiviä suppeammat, säännökset myös henkilötietolakiin (523/1999).

Tietoturvallisuus koettiin tietoteknisenä, yksittäisen koneen tai konehuoneen suojaamisen asiana. Juristeja ei aina koettu legitimeiksi tietoturvallisuudesta keskustelijoiksi. Juristit, varsinkin osa perinteisistä yliopistollisista tutkijoista, taas katsoivat työskentelevänsä arvokkaampien ja pysyvämpien oikeusperiaatteiden kuin teknisten tietoturvallisuusasioiden parissa. Lainvalmistelussa ratkaistiin pragmaattiset ongelmat olemassa olevaan lainsäädännön systematiikkaan istutetuilla säännöksillä. Aika ei ollut vielä kypsä tietoturvallisuuden sääntelyn laajemmalle pohtimiselle.

Tietoturvallisuuslakia ei säädetty mutta tietoturvallisuus oikeudellistui nopeasti

Tietoturvallisuuslakia ei säädetty vaikka eduskunnan oikeusasiamies sitä kannatti. Tietoturvallisuus ja laki –tutkimus osaltaan kuitenkin vauhditti ja osaltaan tuki sitä, että viranomaisten toiminnan julkisuudesta annettuun lakiin (621/1999), julkisuuslaki, otettiin tietoturvallisuutta ja laajemmin hyvää tiedonhallintatapaa koskevat säännökset (JulkL 18 §). Julkisuuslain säännökset käytännössä edellyttävät laajasti tietoturvaluustoimenpiteitä mutta myös järjestelmällistä tietojohdosta. Henkilötietolakiin otettiin EU:n direktiivin toteuttamiseksi ja henkilötietojen suojaa koskevan ajattelun mukaisesti tietoturvallisuutta koskevat säännökset (HenkTietL 32 §).

Tietoturvallisuus oikeudellistui ilman yleistä tietoturvallisuuslakiakin nopeasti. Tietoturvallisuutta koskeviin yleislakeihin kuuluvaksi säädettiin vuonna 2004 kansainvälisistä tietoturvallisuusvelvoitteista annettu laki (588/2004). Merkittäviin tietoturvaluussäännöksiin kuuluvat myös sähköisen viestinnän tietosuojalaki (516/2004) muutoksineen ja laki yksityisyyden suojasta työelämässä (759/2004) eli nk. työelämän tietosuojalaki sekä turvallisuus selvityksistä annettu laki (177/2002). Julkisuuslain nojalla ollaan keväällä antamassa valtioneuvoston asetusta valtionhallinnon tietoturvaluudesta.

Onko tietoturvaluudessa sääntelykierre?

Tietoturvaluuden oikeudellistuminen on sittemmin vain kiihtynyt. Paremmen sääntelyn periaatteiden ja sääntelyn tiedollisen hallittavuuden ja informaatiokustannusten näkökulmasta voidaan kysyä, että onko se oikeudellistunut pulmallisenkin nopeasti. Tänä päivänä tietoturvaluutta koskevat laajasti eri yleis- ja erityislakien säännökset. On laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009), laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009), laki tietoyhteiskunnan palveluiden tarjoamisesta (458/2002), sähköisestä viranomaisasiointista (13/2003). Osa näistä säädöksistä on valmisteltavana muutoksia. Lisäksi tietoturvaluuden kannalta tärkeitä säännöksiä on laajassa joukossa eri sektoreiden rekistereitä ja tietojenkäsittelyä koskevaa erityislainsäädäntöä.

Tietoturvaluutta ohjeistetaan laajasti ja ohjeistajia on monta, osin epävarmoilla toimivaltuuksilla

Lainsäädäntöä täydentävä valtionhallinnon tietoturvaluusohjeistus on myös määrällisesti laajaa. Ohjeistusta ja viestinnän osalta myös määräyksiä eri toimivaltuuksien puitteissa antavat yhtäältä tietosuojavaltuutettu ja toisaalta valtionhallinnon tietoturvaluuden johtoryhmä sekä sähköisen viestintäverkkojen ja laitteiden osalta viestintävirasto, johon sijoittuu myös CERT-FI toiminta. Ohjeistuksen on erilaisten oikeudellisten vaatimusten läpäisemää. Ohjeistuksen ja tietoturvaluustoiminnan oikeudellinen perusta ja sen selvyys vaihtelevat. Ohjeistus on niin laajaa, ettei se ole ainakaan yleisjohton hallittavissa.

Tietoturvaluusohjeisto ja tietoturvaluutta koskevat säännökset muodostavat vaikeasti hahmotettavan ja hallittavan kokonaisuuden

Kokonaisuutena tietoturvaluutta ja sen keskeisiä osa-alueita koskeva lainsäädäntö on vaikeaselkoinen ja monimutkainen kokonaisuus. Onkin syytä kysyä, vastaako se paremmen sääntelyn periaatteita ja erityisesti lainsäädännön selkeyden vaatimuksia. Sama huomio on tehtävissä myös käytännön ohjeistuksesta.

Tietotekniikan muutoksen, aidon verkkoyhteiskunnan ja sen informaatiohallinnon kehittymisen ja tietoturvaluuden nopean oikeudellistumisen ja pirstaloituvan sääntelyn takia ei olekaan yllättävää, että kysymys tietoturvaluuslain tarpeellisuudesta on noussut uudelleen esille. Professori Ahti Saarenpää on valtiovarainministeriölle perusrekistereiden sääntelytarpeista vuonna 2009 tekemässään raportissa ehdottanut tietoturvaluuslain säätämistä. Tietoturvaluuslain säätäminen on yhtenä kysymyksenä esillä keskusteltaessa valtioneuvoston tietoturvaluuden kehittämisestä syksyllä 2009 antaman periaatepäätöksen pohjalta valtionhallinnon tietoturvaluuden johtoryhmän

uutta työsuunnitelmaa vuosille 2010 – 2015. Tietoturvallisuuslakia koskeva kysymys on ollut esillä myös tietosuojavaltuutetun julkisissa pohdintoissa.

Kysyn tässä esityksessä pitäisikö Suomeen säätää tietoturvallisuuslaki. Tietoturvallisuuslain säätämisen tarvetta voidaan ja tulee pohtia seuraavien kolmen eri kysymyksen ja näkökulman kautta:

Mahdollisia perusteita tietoturvallisuudelle

- 1) edellyttävätkö kansainväliset ihmisoikeusvelvoitteet ja niitä toteuttavat Suomen perustuslain perusoikeudet ja perusoikeuksien tulkinta tietoturvallisuuslain säätämistä (*perusoikeusperustelu*)
- 2) onko tietoturvallisuuslain säätämiseksi taloustieteelliset perusteet taloustieteen oikeudelliselle sääntelylle antamien funktioiden ja yhtenä osana oikeudellisen sääntelyn lainsäädännöllisiä perusteita erityisesti kilpailukyvyn kannalta (*taloudellinen perustelu*).
- 3) olisiko tietoturvallisuuslain säätäminen perusteltua ja tarkoituksenmukaista tietoturvallisuuden ohjauksen ja tietoturvallisuustyön yhteiskunnallisen vaikuttavuuden ja toiminnallisen tuloksellisuuden näkökulmasta (*vaikuttavuusperustelu*). Tässä on myös kysyttävä, onko tietoturvallisuudesta tullut sellainen osa yhteiskunnan perusinfrastruktuuria, että siitä pitäisi säätää samalla tavoin kuin monista muistakin perusinfrastruktuuriin kuuluvista asioista on säädetty (*infrastruktuuriperustelu*)

Näiden kysymysten kautta voidaan lähestyä kokoavaa kysymystä siihen olisiko tietoturvallisuutta koskevien säännösten kokoaminen yhteen lakiin perusteltua paremman sääntelyn periaatteiden toteuttamisen näkökulmasta (*paremman sääntelyn perustelu*).

Tarkastelen kysymystä Suomen ja osin suomalaisten yritysten kilpailukyvyn sekä paremman sääntelyn periaatteiden näkökulmasta. Analyysissäni olen päätenyt siihen, että paremman sääntelyn periaatteiden ja kilpailukyvyn näkökulmasta tietoturvallisuuslain säätäminen olisi perusteltua.

Tietoturvallisuuden tekniset ja hallinnolliset ulottuvuudet kehittyvät 2010 –luvulla

Tietoturvallisuus on moniulotteinen ja monitulkintainen asia. Teknisissä tieteissä ja tietotekniikassa tietoturvallisuuden määrittelyä käsitteiden avulla jonkin verran vierastetaan. Tietoturvallisuus ymmärretään tietojenkäsittelyn jatkuvuutena tai koskemattomuutena ja virheettömyytenä – eheytenä – erilaisia uhkia vastaan ja tietoaaineistojen säilymisenä vain niiden käyttöön oikeutettujen käsissä. Tietoturvallisuudelle on kehitetty mittareita. Tietoturvallisuuden mittaamisessa usein seurataan ja mitataan tietojärjestelmien prosesseja.

Tietoturvallisuus ymmärretään johtamisessa ja erityisesti turvallisuusjohtamisessa osaksi laajempaa yritysturvallisuutta, yrityksen tai julkisen toimintayksikön toiminnan, voimavarojen, liike- ja yrityssalaisuuksien sekä henkilöstön suojaamista.

Käytettävyys, eheys ja aitous, luottamuksellisuus sekä jäljitettävyys

Tietoturvallisuus voidaan teknisessä ja johtamisen näkökulmasta lyhyesti määritellä asiaintilaksi, joka tarkoittaa asiantilaa, jossa tiedon ja viestinnän käytettävyyteen, eheyteen, aitouteen (autenttisuuteen) ja luottamuksellisuuteen kohdistuvat riskit on kohtuullisessa määrin hallinnassa eli tietovarantojen ja niiden sisältämän informaation sekä viestinnän käytettävyys, eheys, aitous ja luottamuksellisuus on turvattu. Tietoturvallisuuteen voidaan myös liittää tietojärjestelmässä tehtyjen toimintojen ja tietojen muutosten sekä tietojärjestelmän omien toimintojen jäljitettävyys ja todennettavuus (auditointavuus) ja läpinäkyvyys.

Jäljitettävyys eli
auditoivuus on ihmisoikeusvaatimus

Euroopan ihmisoikeustuomioistuin on viime aikoina oikeuskäytännössään osaltaan korostanut auditoitavuutta yhtenä osana vaatimuksia, joita Euroopan ihmisoikeussopimus asettaa tietojenkäsittelylle ja sen sääntelylle ihmis- ja perusoikeuden yksityiselämän suojaan toteuttamiseksi.

Teknisen ja tietojohdamiseen liittyvän tietoturvallisuuden osalta kiintoisaa on käytettävyyden ja verkottumisen nousu yhä tärkeämmäksi tietotekniikalta, tietojenkäsittelyltä ja viestinnältä vaadittavaksi ominaisuudeksi. Käytettävyyden välttämätön edellytys on tietorakenteiden ja tietojärjestelmien yhteentoimivuus.

Yhteentoimivuus on osa tietojohdamista ja tietoturvallisuudessa korostuva käytettävyyden ulottuvuus

Nykyisen informaatiohallinnon ja verkkoperusteisiin ratkaisuihin paljolti perustuvan tieto- ja viestintäteknikan aikana arkipäivää on ja pitäisi olla tietojen jakaminen ja yhteiskäyttöisyys. Tietojärjestelmät ja tietorakenteet olisi oikeudellisesti, johtamisen näkökulmasta ja teknisesti suunniteltava siten, että jakaminen oikeudellisesti kestäväällä tavalla on mukana arkkitehtuurissa ja sitä koskevissa säännöksissä. Tämä edellyttää yhteentoimivuutta ja edellyttää käyttötarkoitussidonnaisuuksien koodaamista metatietorakenteisiin ja tietojärjestelmien toimintoihin samoin kuin todennettavuuden ja jäljitettävyyden (auditoitavuus) roolin vahvistumista. Tietojohdaminen ja tietojärjestelmien järjestäminen siitä näkökulmasta on välttämätöntä. Tietojohdamisen näkökulmaa tarvitaan myös säädösvalmistelussa ja oikeudellista näkökulmaa ei ole lupa sivuuttaa tietojohdamisessa.

Nykyisen julkisen IT –toiminnan tehokkuuden ja tietojen käytettävyyden suurimpia pulmia on yhteentoimivuuden puutteet. Nämä puutteet aiheuttavat ongelmia ja riskejä tietoturvallisuudelle monella tapaa. Lisäksi yhteentoimivuuden puutteet saattavat vaarantaa esimerkiksi terveydenhuollossa jopa potilasturvallisuuden. Taloudellisesti yhteentoimivuus on myös terveen kilpailun edellytys. Tietoarkkitehtuurissa ja tietojärjestelmäarkkitehtuurissa on siten niin tietojen, tietorakenteiden kuin tietojärjestelmien yhteentoimivuus noussut näin keskeisesti valtiontalouden tarkastusviraston huomion kohteeksi ja tarkastusviraston kertomusten ja eduskunnan tarkastusvaliokunnan mietintöjen pohjalta myös eduskunta on ottanut voimakkaasti kantaa julkisen sektorin tietojärjestelmien yhteentoimivuuden turvaamiseksi.

Valtiontalouden tarkastusviraston tietojärjestelmä- ja ITC –hankkeiden ja ohjelmien sekä yleensä informaatiohallinnon tarkastuksissa on tämän vuoksi ryhdytty kiinnittämään erityistä huomiota myös tietoarkkitehtuurien ja tietojärjestelmäarkkitehtuurien arviointiin yhteentoimivuuden näkökulmasta. Asia on tällä hetkellä erityisen ajankohdainen julkisella sektorilla sosiaali- ja terveydenhuollon valtakunnallisissa tietojärjestelmissä ja niiden integroimisessa osaksi kuntien ja sairaanhoitopiirien ratkaisuja.

Kokoavasti tältä osin voidaan todeta, että yhteentoimivuus on tullut tärkeäksi osaksi ja edellytykset tietoturvallisuuden perinteisiin kriteereihin kuuluvia käytettävyyttä ja eheyttä. Tietoturvaluustyössä on näin siten kiinnitettävä huomiota turvalliseen yhteentoimivuuteen. Yhteentoimivuus puolestaan taloudellisen tehokkuuden edellytys. Yhteentoimivuus täytyy varmistaa monimuotoisilla ratkaisuilla, joissa tarvitaan avoimia ja standardoituja tietorakenteita ja rajapintoja. Sellaisten toteuttaminen on sitten tärkeä julkisen tietojohdamisen tavoite.

Tietoturvaluus on oikeutta turvalliseen identiteettiin

Tietoturvaluus on myös oikeudellinen käsite ja periaate sekä oikeudellinen toimintavelvoite (velvollisuus). Tietoturvaluus voidaan oikeudellisesti ymmärtää yleisellä tasolla informaation, viestinnän ja tietojenkäsittelyn käytettävyyteen, eheyteen, aitou-

teen, luottamuksellisuuteen ja käyttöön sekä toimintojen todennettavuuteen ja avoimuuteen kohdistuvien oikeuksien toteuttamiseksi. Tietoturvallisuus on myös asiantila, jossa nämä oikeudet on vaikuttavalla tavalla turvattu ja toteutuneet.

Tietoturvallisuudesta huolehtiminen kuuluu verkkoyhteiskunnan kansalaisuuteen

Tietoturvallisuus on nykyaikaisessa verkkoyhteiskunnassa myös moraalinen ja eettinen periaate ja velvollisuus. Tietoturvallisuus on perimmäältään yhteisön ja toisen ja tämän oikeuksien ja etujen kunnioittamista tietojenkäsittelyssä ja viestinnässä sekä näiden infrastruktuureissa eli kohtaamisen etiikkaa. Tietoturvallisuudesta huolehtiminen on tämän päivän yhteisöllistä jäsenyyttä – julkisessa keskustelussa paljon puhuttua yhteisöllisyyttä – ja vastuullista kansalaisuutta.

Tietoturvallisuudesta huolehtiminen on Euroopan ihmisoikeussopimuksen vaatimus

Tietoturvallisuuden oikeudellisen sääntelyn kannalta voidaan nähdä muutamia viime kädessä perusoikeuksien tasolla olevia muutoksia. Tietoturvallisuus on vanhastaan ollut Euroopan ihmisoikeussopimuksen käsitteistöllä yksityiselämän suojan yksi välttämätön edellytys. Tämä on 2000 –luvulla tullut hyvin selkeästi todetuksi Euroopan ihmisoikeustuomioistuimen ratkaisuisissa, muun muassa vuonna 2008 annetuissa Suomea koskevista langettavissa tuomioissa asioissa *I v. Suomi* ja *K.U. v. Suomi*. *Euroopan ihmisoikeustuomioistuin on nähnyt tietoturvallisuusjärjestelyt myös osana eri perusoikeuksien tasapainottamista*. Ihmisoikeustuomioistuin on myös arvioinut tietoturvallisuuden monia kantavia periaatteita ja osa-alueita myös lainsäätäjän oikeuden yksityiselämän suojan positiivisina toteuttamisvelvoitteina. Ihmisoikeustuomioistuin on edellyttänyt jatkuvasti arvioitavan myös teknistä ja yhteiskunnallista toimintaympäristöä siten, että lainsäädäntö antaa perusteet tarvittaville tietoturvallisuusjärjestelyille ja muille oikeutta yksityiselämän suojaan toteuttaville järjestelyille. *Tästä perusoikeusperustelun tai perusoikeusvelvoitteen näkökulmasta olisikin tarkasteltava nykyisen lainsäädännön riittävyttä ja ajantasaisuutta*.

Ihmisoikeustuomioistuimen tuomioita ja varsinkin ihmisoikeussopimuksen vanhaa tekstiä – ja samalla myös Suomen perustuslain perusoikeussäännöksiä – luetaessa on pidettävä mielessä, että ihmisoikeustuomioistuimelle oikeus yksityiselämän suojaan sisältää kokonaisen oikeuksien perheen, jotka olennaisilta osin muodostavat laajemman oikeuden yksityisyyteen. Ihmisoikeustuomioistuin on katsonut oikeuteen yksityiselämään kuuluvan myös oikeuden identiteettiin.

Tietoturvallisuus on oikeutta turvalliseen identiteettiin

Ihmisoikeustuomioistuimen oikeuskäytäntöä rohkeasti tulkittaessa voidaan päätyä siihen, että oikeus yksityiselämään sisältää myös *oikeuden turvalliseen identiteettiin*. Tänä päivänä oikeus identiteettiin toteutuu pitkälti myös verkoissa ja edellyttää korkeaa tietoturvallisuuden tasoa. Ihmisoikeustuomioistuimen oikeuskäytännön valossa onkin perusteltua nähdä yksilöllä olevan oikeuden tietoturvallisuuteen ja turvalliseen identiteettiin sekä identiteettiään koskevaan itsemääräämiseen. Yhdessä nämä ovat perusta yksilön kunnioitukselle ja koskemattomuudelle, oikeudelle integriteettiin.

Identiteettivarkaudet ovat tulossa merkittäväksi riskiksi Suomessa

Suomen tilannetta arvioitaessa on todettava, että identiteettivarkaudet ovat vahvasti nousussa Suomessakin olennaiseksi jokaista koskettavaksi tietoturvallisuusriskiksi. Kehitys meillä seuraa samaa polkua kuin Yhdysvalloissa. Olisikin pikaisesti arvioitava, antaako Suomen lainsäädäntö riittävästi suoja identiteettivarkauksia vastaan ja suojataanko meillä riittävästi sähköisen identiteetin turvallisuutta. Myös viranomaisten resurssit (henkilöresurssit, osaaminen) käsitellä ne tehokkaasti on turvattava.

Tietoturvallisuuden kannalta olennaista tässä kehityksessä on siis se, ettei tietoturvallisuus näin ole enää ainoastaan oikeuden ja oikeuksien toteuttamisen tekninen edellytys. Tietoturvallisuudesta itsestään on tullut oikeus ja kantava osa oikeutta turvalliseen identiteettiin ja integriteettiin.

Vastaava kehityskulku on nähtävissä oikeuden omaisuuden suojaan ja tietoturvallisuuden välisissä suhteissa. Suomessa omaisuuden suoja käsittää myös immateriaaliset oikeudet, esimerkiksi tekijänoikeudet. Euroopan unionin perusoikeusperuskirjassa suojataan erikseen perusoikeuksina myös tekijänoikeuksia. Liikesalaisuudet ovat myös omaisuuden suojan piiriin kuuluvia ja siten esimerkiksi julkisuuslain 24 §:ssä olevat yksityistä liikesalaisuutta turvaavat salassapitosäännökset ja julkisuuslain 18 §:n hyvän tiedonhallintatavan alaan kuuluvat tietoturvaluustoimenpiteet ja julkinen tietojohdaminen turvaavat osaltaan perusoikeuden reaalista toteutumista. Oikeudet kohdistuvat yhä enemmän immateriaaliin, digitaalisessa muodossa tai tietoverkoissa oleviin objekteihin. Tietoturvallisuuden merkitys reaalisen oikeuden elementtinä korostuu. Mutta yksityisoikeudellisessa kehityksessä tietoturvallisuudesta ja oikeudesta ryhtyä tarpeellisiin turvaluustoimenpiteisiin sekä toisaalta oikeudesta vaatia tietoturvallisuutta alkaa tulla jo itsenäinen oikeutensa. Tämä näkyy muun muassa tekijänoikeusjärjestelmässä, jossa oikeus teknisiin suojakeinoihin sekä oikeus teknisiin hallintajärjestelmiin tulevat osaksi tekijänoikeusjärjestelmää ja eri oikeuksien tasapainoa samoin kuin oikeudelliseen sääntelyyn perustuvaa hallintajärjestelmää. Tästä on hyvä analyysi Viveca Stillin väitöskirjassa DRM och upphovsrättens obalans (2007).

Julkisoikeudellisissa suhteissa tietoturvallisuus on nykyaikaisessa hallinnossa osa lainalaisuusperiaatetta. Julkisen vallan, hallinnon ja palvelutuotannon infraskruktuureihin kohdistuvia oikeudellisia laatuvaatimuksia. Tämä on tullut vahvasti esille eduskunnan oikeusasiamiehen antamissa ratkaisuisissa.

Tietoturvallisuuden voidaan nykyisin katsoa olevan informaatio-oikeudellinen ja ICT-oikeudellinen yleinen oikeusperiaate. Sille löytyy laajalti institutionaalista tukea. Lainsäätäjän näkökulmasta kysymys onkin, onko oikeustila riittävän selkeä.

Tietoturvallisuudesta on tullut julkishyödyke

Tietoturvallisuuden taloudelliset ominaisuudet sekä taloustieteelliset näkökulmat tietoturvallisuuteen ovat tietoturvallisuutta koskevan lainsäädännön ja tietoturvallisuuden oikeudellisen ohjauksen kannalta erittäin tärkeä kysymys. Tietoturvallisuus on nykyaikaisessa talouselämässä keskeisten tuotantotehtävien, informaation, tiedon ja viestinnän satavuuden ja käytettävyyden edellytys. Tietoturvallisuus on nähtävissä myös hyödykkeenä. Tietoturvallisuus on ollut yksityinen hyödyke ja sitä edustavat monet markkinoilla myytävät tietoturvaluusuratkaisut ja palvelut.

Mutta 2000-luvulla on tietoturvallisuuden taloudellisessa luonteessa on tapahtunut tietoturvaluusulainsäädännön pohdinnan kannalta olennaisen tärkeä muutos. Tieto- ja viestintäteknikan kehityksen ja verkkoyhteiskunnan muodostumisen myötä tietoturvaluudesta on tullut laajalti myös julkishyödyke.

Tieto- ja viestintäteknologia ja tietoverkot ovat taloustieteellisesti yleiskäyttöisiä teknologioita. Tieto- ja viestintäteknologian tuottavuutta ja innovaatioita edistävät vaikutukset toteutuvat pitkälti viestinnässä ja tietoverkkojen kautta. Niinpä arjen tietoyhteiskuntamme tai kankeammin ubiikkiyhteiskunta onkin lisääntyvässä määrin täynnä verkottunutta, toisten laitteiden ja verkkojen kanssa viestivää tai viestimään kykenevää tietotekniikkaa. Suurin hyöty tästä tekniikasta saadaan hyödyntämällä juuri verkottumisominaisuutta ja verkon tarjoamaa kapasiteettia. Hyvänä esimerkkinä tietotekniikan kehityksestä tässä suhteessa on niin sanotut pilvi-ratkaisut (cloud computing). Pilvi-ratkaisujen rinnalla haasteena ovat perinteisemmät mutta hyvin vaikeat ulkoistamisen tietoturvaluus- ja tietosuojariskit. Tietojenkäsittely ei ole enää rajatussa organisaati-

Tieto- ja viestintä-
verkoissa tietoturvaluusuriskit ulottuvat kolmansiin ja muodostavat systeemisriskejä

ossa tapahtuvassa keskustietokoneessa tapahtuvaa eikä yksin erillään toimivissa henkilökohtaisissa tietokoneissa tapahtuvaa. Tieto- ja viestintäteknikka 2010 –luvulla koostuu monikanavaisista, konvergoituneista eri tavoin älykkäistä päätelaitteista, jotka ovat yhdistyneitä joustavasti ja ketterästi sekä suuriin palvelinkoneisiin että toisiin yksittäisiin koneisiin.

Tieto- ja viestintäteknologian verkottuneisuudesta johtuu, että verkon saatavuus ja käytettävyys ovat tehokkaiden toimintojen ja systeemin toimivuuden edellytys. Samalla tämä muuttaa tietoturvallisuuden luonnetta. Tietoturvallisuus ei enää voi olla yksittäisen organisaation tai yksittäisen henkilön rajatun laitteen riskienhallintaa vaan on ajateltava myös kokonaisuutta. Kulunutta mutta viisauden sisältävää sanontaa käyttäen verkon turvallisuus on yhtä hyvä tai heikko kuin sen heikoimman lenkin turvallisuus. Turvallisuudeltaan älykkäässä verkossa asia ei ole näin vaan verkko kykenee monitorimaan omaa turvallisuutta ja tarjoamaan siten kokonaisuutena parempaa turvallisuutta kuin mitä olisi saavutettavissa yksittäisen toimijan tai päätelaitetason turvallisuusratkaisuilla. Verkon yksittäisen kohdan haavoittuvuus on kuitenkin merkittävä koko verkon haavoittuvuus. Riskienhallintaa ja turvallisuutta on ajateltava näin kokonaisuudessa.

Rahoitusmarkkinoiden kriisissä vastapuoliriskit kumuloituivat systeemiriskin partaalle

Riskienhallinnan teorian ja käytännön oppien näkökulmasta tietoturvallisuudessa käy samoin kuin mitä tapahtui rahoitusmarkkinoiden sääntelyssä ja rahoituslaitosten riskienhallinnassa. Kansainvälisten rahoitusmarkkinoiden viimeisin kriisi ja kriisin taustalla olevat riskienhallinnan rakenteelliset ja kognitiiviset pulmat sisältävätkin oppia, joka kannattaa ottaa pohdittavaksi myös tietoturvallisuuden yhteydessä.¹

Rahoitusmarkkinoiden riskienhallinnan sääntely ja riskienhallinta oli keskittynyt ennen nyt koettua kriisiä pitkälti yksittäisten yritysten riskien hallintaan. Sopimuksiin perustuvia vastapuoliriskejä tarkasteltiin niin ikään mikrotasolla osana yrityksen sopimustenhallintaa ja etupäässä yksittäisessä sopimussuhteessa. Vastapuoliriskien eli vastapuolen maksukyvyttömyyden tai suoritushäiriöiden kumuloitumista ja sen heijastumista myös makrotasolle ei sen sijaan huomattu riittävästi tarkastella. Vastapuoliriskien kumuloituminen ja toteutuminen johtivat kuitenkin rahoitusjärjestelmän systeemiriskin partaalle eli koko kansainvälinen rahoitusjärjestelmä oli lähellä romahtamista. Vastapuoliriskit ja niiden puutteellinen hallinta muodostivat näin koko järjestelmää uhanneen systeemiriskin. Rahoitusmarkkinoiden vakaus ja saatavuus puolestaan ovat nykyaikaisessa kansainvälisessä taloudessa julkishyödyke.

Tietoturvallisuudessakin riskit voivat kumuloitua ja tietoturvallisuus ei ole enää vain yksilön tai organisaation oma asia

Samalla tavoin tieto- ja viestintäverkoissa ja verkottuneissa tai verkottumaan kykenevissä tietojärjestelmissä yksittäisten tietoturvallisuusriskien kumuloituminen muodostaa jopa systeemiriskin tai ainakin useita toimijoita koskevan merkittävän tietoturvallisuusriskin. Esimerkkinä tästä voidaan mainita boot –verkkojen kautta tehtävät palvelunestohyökkäykset tai luotettavina pidettyjen verkkosivujen haavoittuvuuksien hyödyntäminen haittaohjelmien levittämiseen ja laitteiden kaappaamiseen. Oikeudellisen sääntelyn tarpeiden kannalta merkityksellistä tässä on se, että muillakin kuin yksittäis-

¹ Valtiontalouden tarkastusvirasto johtaa kansainvälisten rahoituskriisien välttämistä sekä vaikutusten minimoimista pohtivaa kansainvälistä työryhmää Yhdysvaltain liittovaltion ylimmän tarkastusviraston Government Accountability Office GAO:n johtamassa kansainvälisessä ylimpien tarkastusviranomaisien yhteistyöryhmässä (INTOSAI Task Force on Global Financial Crises). Tämän johdosta valtiontalouden tarkastusvirastossa tarkastellaan kansainvälisten rahoitusmarkkinakriisien mekanismeja ja siten, miten ylimmän ulkoisen tarkastuksen avulla tilivelvollisuutta ja vastuunalaisuutta voitaisiin parantaa. Yhdysvaltain liittovaltion tarkastusvirasto GAO on Yhdysvaltain rahoitusmarkkinoiden vakauttamista ja pankkien pelastamista koskevan ns. TARP –lainsäädännön mukaan Yhdysvalloissa viranomainen, jonka tulee säännöllisesti raportoida vakauttamisen onnistumisesta (vakauttamisen vaikuttavuudesta).

sellä verkon osapuolella ja tämän välittömällä sopimuskumppaneilla on perusteltu vaade näin kumppaneiden tietoturvallisuuden tasoon ja tietoturvallisuudesta huolehtimiseen. Taloustieteen Nobelin vuonna 2009 saaneen Oliver E. Williamsonin mukaan oikeudellisen sääntelyn ja johtamisen yhtenä tärkeänä tehtävänä on antaa hallintavälineitä. Uudessa teknisessä ja riskien todellisuudessa perinteiset hallintavälineet, esimerkiksi sopimus ja sopimusoikeus, eivät enää ole riittäviä. Tietoturvallisuuden sääntelyssä vallitsee siten sama tilanne kuin rahoitusmarkkinoiden vastapuoliriskien ja systemiriskien sekä niiden kumuloituvien vaikutusten hallinnassa.

Tietoturvallisuuden sääntelyn näkökulmasta kiinnostavaa on myös havaita tietotekniikan ja organisaatiomuotojen välinen yhteys. Talouden ja tekniikan historian ja organisaatioiden muodon välillä vaikuttaisi olevan säännöllinen yhteys. Organisaatiomuotojen ja oikeuden välillä taas on suora yhteys Williamsonin teorian osoittamalla tavalla; oikeus on yksi hallintavälineistä ja siten organisaation murrokset merkitsevät väistämättä myös oikeudellisen sääntelyn tapojen muutoksia (sääntelyparadigman muutos). Nykyinen hajanainen tietoturvallisuuden sääntely perustuu pääosin ajatuksellisesti keskenään erillisten tietoverkkojen ja henkilökohtaisen tietokoneen tekniikan. Laaja-alainen konvergenssi ja verkottuminen eivät vielä riittävästi näy sääntelymallissa.

Milloin oikeudellinen sääntely on taloustieteellisestä näkökulmasta perusteltua

Sääntelyinnokkuutta varottava

Tietoturvallisuuden kaltaisen teknisen ja taloudellisen asian sääntely oikeudellisesti tai rullinnollinen ohjaus ja sääntely eivät ole voi olla itsetarkoitus. On jopa varottava hyvää tarkoittavasta, liiaksi tiettyyn muottiin tai teknologiaan tai teknisen ratkaisun edistämiseen perustuvasta lainsäädännöstä. Nämä saattaisivat lyhyellä tähtämellä vaikuttaa tehokkailta ja kustannuksia säästävilä. Vaikeutena on, että lainsäätäjän kautta tapahtuva, liian pitkälle menevä keskittetty suunnittelu tukahduttaa tai rajoittaa innovaatioita ja muutosta ja näin heikentää dynaamista tehokkuutta. Tämä johtuu jo siitä, ettei lainsäätäjällä ole riittävästi informaatiota ja tietoa kaikista yksittäisistä tilanteista. Informaation taloustiede perustelee näin yleislainsäädäntöä ja teknologianeutraalia lainsäädäntöä. Dynamiikan kannalta lainsäädännön roolina on muodollisten pelisääntöjen ja mahdollisimman ennakoitavien toimintaedellytysten luominen. Lainsäädäntö on esimerkiksi F.A. Hayekin mukaan legitimiä silloin, kun se on enemmän muodolliseen yhdenvertaisuuteen ja oikeudenmukaisuuteen perustuvaa ja ennustettavaa yleislainsäädäntöä. Lainsäädäntö on perusteltua esimerkiksi toisia loukkaavien väärinkäytösten torjumiseksi tai reilun kilpailun edellytysten luomiseksi.

Lainsäätäjällä on vakava informaatio-ongelma

Tarkemmin taloustieteelliset perustelut sääntelylle voidaan tiivistetysti esittää seuraavasti:

Taloustieteellisiä perusteluita oikeudelliselle sääntelylle

- ulkoisvaikutusten hallinta ja erityisesti kielteisten ulkoisvaikutusten hallinta
- julkishyödykkeiden tuottaminen ja moraalikadon välttäminen tai hallinta
- kilpailun puutteiden tai vastaavien markkinahäiriöiden korjaaminen
- markkinoiden ja niiden pelisääntöjen perustaminen
- epätäydellisen informaation aiheuttamien informaatio-ongelmien hallinta. Varsinkin luottamushyödykkeissä sääntely voi olla toimiva keino korjata informaatio-ongelmia. Luottamushyödykkeet poikkeavat niin sanotuista etsintähyödykkeistä siinä, ettei tuotteen laatuominaisuudet ole helposti havaittavissa hinnasta ja tuotettava ennen sen käyttöä ulkoisesti vertailemalla.

Tietoturvallisuuden muuttuminen julkishyödykkeeksi perustelee sääntelyä

Tässä tarkastelussa tietoturvallisuuden muuttuminen julkishyödykkeeksi ja ubiikin verkkoyhteiskunnan riskien ja niiden muodostamien kielteisten ulkoisvaikutusten kohdentuminen kaikille on selkein lainsäädännön taloustieteellinen perustelu. Tieto-

turvallisuudessa on osaksi myös kyse luottamushyödykkeestä, jossa yksittäisten toimijoiden mahdollisuudet testata kaikkia tuotteita ja palveluita ovat erinäisistä syistä rajoitettuja. Tietoverkkoympäristössä tietoturvallisuusriskien hallinnassa voi esiintyä myös moraalikatoa.

Tietoturvallisuus
psykologisen talous-
tieteen näkökulmas-
ta

Täydentävän näkökulman oikeudellisen sääntelyn tarpeeseen ja mahdollisuuteen tarjoaa psykologinen taloustiede (behavioral economics) ja sen pohjalta psykologinen oikeustaloustiede (behavioral law and economics). Lähtökohtana tässä ovat ihmisen kognitiiviset ominaisuudet ja niistä johtuvat rationaalisuuden rajoitteet. Rationaalisuuden rajoitteet monilta osin "vääristävät" käyttäytymistä verrattuna rationaalisen käyttäytymisen ideaaliin. Lainsäädäntö on yleensä vahva viesti oikeasta ja väärästä. Käyttäytymiseen ja arvostuksiin voidaan näin vaikuttaa ainakin jossain määrin oikeudellisen sääntelyn avulla. Sääntelyn avulla voidaan rajoitetussa määrin pakottaa tietoisuuteen myös sellaisia riskejä, jotka ihmisellä on kognitiivisten ominaisuuksiensa johdosta taipumus hylätä tai aliarvioida. Ihmisillä on yleensä taipumus esimerkiksi aliarvioida tavalliseen arkeen sisältyviä riskejä.

Tietoturvallisuus on ala, jossa yksityisten toimijoiden tapa hahmottaa ja ymmärtää riskejä on erilainen. Riskien aliarviointi johtuu usein omasta laiskuudesta ja mukavuudenhalusta. Varsinkin verkkoympäristössä heikomman turvallisuustason muille aiheuttamia uhkia ja riskejä ei välttämättä mielletä. Parhaimmillaan tietoturvallisuuslainsäädännöllä voidaan osaltaan tukea tietoturvallisuusriskien hahmottamista ja sisäistämistä kunkin toimijan omaan toimintaan. Yleinen tietoturvallisuuslaki voisi auttaa sen mieltämistä, että tietoturvallisuus on jokaisen velvoite.

Lailla ei kuitenkaan voida rajoituksetta vaikuttaa käyttäytymiseen. Liian laaja ja heikosti vaikuttava sääntely ja säädöskierre pikemminkin heikentävät lain mahdollisuuksia korjata riskien arvioinnin virhetaipumuksia. Tietoturvallisuutta koskevassa sääntelyssä onkin arvioitava tarkasti sääntelyn ja muiden ohjauskeinojen käyttäytymisvaikutuksia.

Kilpailuvyyn vaatimukset tietoturvallisuuden sääntelylle

Kilpailukyky on liitettävissä markkinoilla tapahtuvaan toimintaan. Kilpailukykyinen yritys pystyy saavuttamaan markkinoita tuotteilleen eli pärjää kilpailussa. Viime kädessä kilpailukykyisen yrityksen ominaisuus on tuottaa ajallisesti riittävän kestävällä tavalla rahavirtaa omistajilleen – joko omistuksen arvon nousuna tai yrityksen tuottamana osinkona tai muuna tulona ja taloudellisena etuutena.

Kilpailuvyyn liittäminen ominaisuutena kansantalouteen tai valtioon on jo monitahoisempi asia – kilpailukyky kun on lähtökohtaisesti markkinoilla pärjäämistä kuvaava ominaisuus. Valtion tai kansantalouden kilpailukyky voidaan ymmärtää yhtäältä kansantalouden tai valtion pärjäämisestä kansainvälisessä valtioiden ja kansantalouksien kilpailussa (esimerkiksi verokilpailussa tai kilpailuissa osaavasta työvoimasta, innovaatioista, sijoituksista), jolloin ajatus markkinoista tulkitaan myös laajasti ja käsitettävän julkisten toimijoiden ja jopa aatteiden välisiä suhteita. Suppeammin kansantalouden (ja valtion) kilpailukyky voidaan ymmärtää kansantalouden menestykseksi saada aikaan taloudellista kasvua ja houkutellessa taloudellista toimeliaisuutta piiriinsä. Bruttokansantuotteen kasvu ja kehitys pitkässä aikasarjassa on siten edelleen yksi parhaimmista mittareista, joilla kansantalouden kilpailukykyä voidaan mitata.

Bruttokansantuotteen pitkäaikaisella kehityksellä mitattu kansantalouden kasvu itse asiassa muodostuu summana kansantalouteen kuuluvien talousyksiköiden, joiden kes-

Milloin kansantalouden voidaan sanoa olevan kilpailukykyinen?

keisen joukon muodostavat yritykset, luomista virroista ja varannoista. Kansantalouden kilpailukyky onkin sen yksittäisten taloudellisten toimijoiden kilpailukyvyn summa. Toisaalta kansantalouden tila vaikuttaa olennaisellakin tavalla sen yksittäisten taloudellisten toimijoiden kilpailukyvyn edellytyksiin.

Kilpailukykyä mitataan usein myös erilaisilla useista muuttujista kootuilla yhdistelmä-tunnusluvuilla (komposiitti-indikaattoreilla). Näitä ovat esimerkiksi kilpailukykyindeksit. Kyseiset indeksit kuvaavat seikkoja, joiden on perusteltu olevan tai joiden ainakin arvioidaan olevan menestyvän yritystoiminnan edellytyksiä. Kilpailukykyindikaattoreiden ja yritysten sijoittumisen/yrityksyyden tai suorien sijoitusten suuntautumisen tai kansantalouden vaihtosuhteen (vaihtotase) välillä ei kuitenkaan vallitse lineaarinen yhteys. Monet kilpailukykyindikaattorit ennustavat puutteellisesti tai jopa heikosti bruttokansantuotteen kehityksellä tai sijoitusten suuntautumisella taikka vaihtotaseella mitattua kilpailukykyä.

Paremmen sääntelyn periaatteiden toteutuminen ja parempi kilpailukyky näyttäisivät olevan yhteydessä toisiinsa

Kansantalouden tasolla tarkastellun kilpailukyvyn ja hyvän sääntelyn eli niin sanotun paremmen sääntelyn periaatteiden mukaisen sääntelyn välinen yhteys on niin ikään epäselvä ja monitulkintainen. Eri tutkimusten ja tarkasteluiden perusteella näyttäisi kuitenkin siltä, että instituutiot ja niiden laatu ovat merkittäviä historiallisen taloudellisen kasvun eroja selittäviä tekijöitä. Innovaatiot ja niiden aiheuttama tuottavuuden kasvu on merkittävä talouskasvun taustalla oleva seikka. Makrotason tarkasteluissa näyttäisi myös olevan niin, että paremmen sääntelyn periaatteiden mukaisella sääntelyllä ja toimivalla oikeusvaltiolla näyttäisi olevan positiivinen yhteys taloudelliseen kasvuun ja siten kilpailukykyyn. Paremmen sääntelyn ja kansantalouden kasvun ja sen ilmentämän kilpailukyvyn välillä näyttäisi näin olevan korrelaatio. Mutta mistä se syntyy? Korrelaation perustana olevat kausaalisuussuhteet ovat moninaisia ja osin kiistanalaisia.

Kilpailukyvyn parantamisen ja paremman sääntelyn välistä yhteyksiä

Jos kansantalouden menestyksen voidaan ajatella johtuvan innovaatioiden ja niiden hyödyntämisen ansiosta syntyvästä tuottavuuden lisäyksestä ja yleensä kansantalouden talousyksiköiden menestyksestä, voidaan karkeasti hahmotella seuraavia näkökohtia kilpailukyvyn ja paremmen sääntelyn välisestä suhteesta:

1. Hyvä sääntely vähentää yritysten ja taloudellisten toimijoiden riskiä ja riskipreemioita ja siten kynnystä osallistua taloudelliseen toimintaan tai rajoitteita harjoittaa sitä
 - a. hyvä sääntely ja toimiva oikeusvaltio luo vakautta ja ennustettavuutta toimintaympäristöön ja oikeussuhteisiin ja siten sopimussuhteisiin
 - b. hyvä sääntely ja toimiva oikeusvaltio luo turvallisuutta
2. Hyvä sääntely vähentää taloudellisten toimijoiden kustannuksia tai pitää kustannukset riittävän pieninä. On tosin tilanteita, joissa tehokkaan riskien hallinnan kannalta on toivottavaakin aiheuttaa virheelliset kannustimet tai kielteiset ulkoisvaikutukset korjaavia kustannuksia. Hyvän sääntelyn kustannuksia vähentävä vaikutus ilmenee muun muassa:
 - a. talouden toimijoille ei aiheudu julkisten velvoitteiden toteuttamisesta tarpeetonta hallinnollista taakkaa.
 - b. talouden toimijoille ei aiheudu sääntelyyn sopeutumisesta tai oikeuden soveltamisesta oppimiskustannuksia tai tarpeettomia toimeenpano- ja sopeutumiskustannuksia. Monimutkainen ja tekniseen kehitykseen nähden pulmallisessa suhteessa olevat säännökset aiheuttavat jatkuvasti ajanhukkaa ja kustannuksia soveltamisessa
 - c. hyvä sääntely ei estä tehokkaampien ja tuottavuutta lisäävien innovaatioiden käyttöä

3. Hyvä sääntely turvaa ja edistää markkinoille pääsyä ja markkinoilla toimimista. Markkinoille pääsyä edistävät kilpailuoikeudellisten normien lisäksi esimerkiksi standardointi ja todistukset standardien ja vaatimusten mukaisuudesta. Esimerkiksi kansainvälisistä tietoturvaluusvelvoitteista annetun lain mukaiset turvallisuusluokitukset ja –sertifikaatit ovat markkinoille pääsyä helpottavia välineitä.
4. Hyvä sääntely turvaa keskeisten tuotannontekijöiden saatavuutta ja dynaamista tehokkuutta edistäviä innovaatioita. Hyvä sääntely kannustaa osaamisen, innovaatioiden ja niitä koskevan tiedon leviämiseen. Osaava henkilöstö on näin yksi kilpailukykytekijä
5. Hyvä sääntely edistää julkisen talouden kestävyttä ja siten julkisen talouden rahoittamisesta pitkällä tähtäimellä taloudellisille toimijoille koituvaa rasitetta ja sen riskiä. Julkisen talouden kestävyttä parantavia toimia ovat erityisesti toiminnan vaikuttavuutta, taloudellisuutta ja tuottavuutta parantavat järjestelyt.
6. Hyvä sääntely edistää resurssien ja kustannusten taloudellisesti tehokasta jakautumista taloudessa. Tämän vaikutus taloudelliseen toimintaan tapahtuu yksittäisten toimijoiden epävarmuuden ja kustannusten suhteutumisen optimaalisella tasolla kautta.

Tietoturvaluusussääntely ja kilpailukyky

Tietoturvaluusussääntely olisi sijoitettava edellä karkeasti hahmotetulle kartalle hyvän sääntelyn ja kilpailukykyyn välisestä suhteesta. Onkin pohdittava, missä määrin toisenlainen tietoturvaluusussääntely näin parantaisi markkinoille pääsyä, alentaisi riskejä ja riskipremioita sekä alentaisi kustannuksia sekä pohdittava, miten ja minkälainen sääntely voisi saada aikaan yllä olevassa katsannossa myönteisiä, taloudellista toimeliaisuutta, tehokkuutta ja tehokasta kustannusten ja riskien jakoa koskevia käyttäytymisvaikutuksia.

Hyvä tietoturvaluusuden yleinen taso edustaa vakautta ja ennustettavuutta

Tässä tyydyn esittämään joitakin lyhyitä luonnehdintoja. Tietoturvaluusuriskien kustannusvaikutukset kasvat ja tietoturvaluusuriskit ovat nousseet merkittäviksi. Siten mahdollisimman tehokas ja vaikuttava tietoturvaluusustyö alkaa olla yhä painavampi osa toimintaympäristön ennustettavuutta ja turvallisuutta sekä oikeussuhteidenkin kautta.

Tietoturvaluusussääntely ei saa aiheuttaa tarpeettomia hallinnollisia tai sopeutumiskustannuksia

Tietoturvaluusussääntely ei saa aiheuttaa tarpeettomia kustannuksia ja hallinnollista taakkaa. Tässä onkin yritysten kannalta huonosti harkitun tietoturvaluusulainsäädännön riski. Se voi aiheuttaa merkittäviä kustannuksia ja siten heikentää yritysten kilpailukykyä. Tietoturvaluusussääntely voi olla merkittävä pulma myös silloin, kun se estää parempien tai kansainvälisessä vaihdannassa tarvittavan korkeamman tietoturvaluusuden tason vaatimisen tai käyttämisen tai tosiasiallisesti ohjaa tai vakiinnuttaa tietoturvaluusuden liian heikolle tasolle. Valtiontalouden tarkastusvirasto on kritisoinut tästä näkökulmasta valtionhallinnon tietoturvaluusuden tasojen määrittelyhanketta hallinnollisen ohjauksen kautta. Vaadittava tietoturvaluusuden perustaso on tullut käytännössä määritetyksi liiaksi pienimmän yhteisen nimittäjän eli heikoimman mukaan.

Nykyinen laaja ja osin vaikeaselkoinen sekä käytännössä vain tiettyihin teknisiin ratkaisuihin ajattelumalliltaan kiinnittyvä sääntely aiheuttaa kuitenkin myös merkittäviä soveltamis- ja oppimiskustannuksia. Paremman sääntelyn periaatteiden mukaan kootummalla ja määrältään vähäisemmällä lainsäädännöllä päästäisiin näin alhaisempiin soveltamisen ja ymmärtämisen kustannuksiin. Varsinkin PK-yritysten ja myös pienten julkisten toimintayksiköiden kannalta nykyistä laajempi ja helpommin ymmärrettäv-

sä oleva tietoturvallisuuden ja tietohallinnon ohjeistus ja standardointi auttaisivat kustannusten pienentämisessä ja tietoriskien paremmassa hallinnassa.

Yhteentoimivuus ja yhteenliitettävät, avoimet rajapinnat ja tietorakenteet edistävät markkinoille pääsyä ja kilpailua

Markkinoille pääsyn ja siellä toimimisen kannalta olennaista on luotettavuutta ja turvallisuutta koskevat sertifikaatit. Niiden osalta nykyinen lainsäädäntö antaa liian vähän tai liian suppeasti toimintamahdollisuuksia muun muassa yritysten henkilöstön turvallisuusluokituksen tai yrityksen turvallisuustasoa koskevien sertifiointien osalta. Markkinoille pääsyn kannalta oleellista on myös yhteentoimivuus. Sen turvaamisessa tarvitaan oikeudellisia säännöksiä ja niitä täydentämään yhteentoimivuuden standardeja. Yleensäkin informaatio-oikeudellisessa ja ICT-infrastruktuurin sääntelymallissa tarvitaan lainsäädännön, standardien ja käytäntöjen yhdistelmää.

Jos lainsäädännöllä ja siihen perustuvalla ohjausmallilla pakotettaisiin nykyistä laajemmin edes julkisen sektorin tietojärjestelmissä avoimiin rajapintoihin ja yhteentöimiviin tietorakenteisiin ja tietojärjestelmiin, olisi mahdollista pilkkoa tieto- ja järjestelmäarkkitehtuureissa nykyiset suuret järjestelmät pienempiin osiin. Tämä antaisi enemmän mahdollisuuksia pienille ja keskisuurille yrityksille päästä ohjelmistomarkkinoille. Tietoturvallisuus ja ohjelmistoturvallisuutta ja arkkitehtuurin turvallisuuden vaatimustenmukaisuutta koskevat virallisen tahon myöntävät sertifiointit parantaisivat niin ikään pienempien yritysten markkinoille pääsyä. Markkinoille tulon uhka taas on tärkeimpiä innovatiivisuutta ja siten dynaamista tehokkuutta ylläpitäviä mekanismeja. Julkisen sektorin tietojärjestelmähankkeissa valtiontalouden tarkastusvirasto taas on todennut isojen, oligopolistisesti käyttäytyvien IT-yritysten kapseloidun liiketoimintamallin aiheuttavan lisäkustannuksia ja tehokkuustappioita.

Hyvä sääntely edistää ja suojaa tehokkaasti yritysten tärkeimpiin tuotannontekijöihin kuuluvan tiedon ja osaamisen sekä niitä koskevien yrityssalaisuuksien säilymistä. Henkilöstön luotettavuus ja turvallisuus ovat osa näitä. Nämä näkökohdat olivatkin Lex Nokian nimellä tunnetun sähköisen viestinnän tietosuojalain muutoksen taustalla. On kuitenkin kysyttävä, onko nykyinen useista laieista koostuva kokonaisuus oikeudellisesti ja taloudellisesti paras mahdollinen. Epäilisin, että ei. Laki on liian vaikea ja löytyy liian useista säädöksistä.

Kansalaisen näkökulma kansantalouden kilpailukyyn ja tietoturvallisuuden sääntelyn väliseen suhteeseen

Tietoturvallisuus on teknisten, johtamisen ja hallinnon sekä asiaan vihkiytyneiden oikeuden asiantuntijoiden aluetta. Kansalaisen näkökulma usein puuttuu. Kansalaisen näkökulmalla on myös selkeä ja vahvistuva yhteys kilpailukyyn. Osaavan henkilöstön saatavuus on kansainvälinen kilpailutekijä. Tässä arjen turvallisuus ja mahdollisuus hyvään elämään on merkittävä.

Tietoturvallisuus kuuluu hyvään elämään

Turvallisuus kuuluu hyvään elämään. Ihminen kaipaa hyvää elämää. Suomen perustuslain 1 §:n 1 momentti sisältää merkittävän ja radikaalin ajatuksen oikeudellisen sääntelyn ja valtiovallan roolista: valtiosääntö turvaa ihmisarvon loukkaamattomuuden ja yksilön vapaudet ja oikeudet sekä edistää oikeudenmukaisuutta yhteiskunnassa. Tämä on nykyaikaisessa länsimaisessa, liberaalissa oikeusvaltiossa valtion ja oikeusjärjestyksen perustehtävä.

Elämme arjen verkkoyhteiskunnassa. Tieto- ja viestintäteknikka ja tietovirrat ovat näkyvästi ja näkymättömästi kaikkialla läsnä. Näin arjen turvallisuuteen ubiikkiyhteiskunnassa kuuluu, että tietoturvallisuutta ja sen mukaista oikeutta identiteettiin ja viestintään suojataan niin oikeudellisesti että käytännössä. Digitaalinen minä tai viestin-

tämme ei saa olla jatkuvasti uhattuna ja siten voimakkaita epäoikeudenmukaisuuden tunteita herättävän kokemuksen lähteenä. Digitaalisen identiteetin turvallisuus on osa turvallisuuden ja turvallisuuden tunteen perhettä.

Mistä tietoturvaluuslaissa voitaisiin tai pitäisi säätää

Tietoturvaluuslaista keskustelu vaikuttaa kovin teoreettiselta jos samalla ei ole ajatusta siitä, mistä tietoturvaluuslaissa pitäisi säätää.

Tietoturvaluuslain valmistelussa ja säätämisessä lähtökohdaksi on hyvä nykyinen oikeudellinen traditio ja sääntely. Tietoturvaluuslain perusrunko saadaan jo olemassa olevien lakien keskeisten periaatteiden kokoamisesta nykyistä paremmin paremman sääntelyn periaatteita vastaavaksi ja tekniikkaneutraalimmaksi kokonaisuudeksi. Tietoturvaluuslakiin tulee näin keskeistä sisältöä muun muassa seuraavien säännösten pohjalta:

- henkilötietolain 32 §:n tietoturvaluusvelvoite ja eräät muut tietoturvaluusvelvoitteita koskevat hyvän tietojenkäsittelytavan säännökset sekä tietoturvaluusvelvoitteita koskevat käytännösäännöt
- julkisuuslain 18 §:n hyvää tiedonhallintatapaa koskevat säännökset ja erityisesti tietoturvaluusvelvoitteita ja yhteentoimivuutta koskevat säännökset
- sähköisen viestinnän tietosuojalain yleisesti kaikkeen viestintään sovellettavat periaatteet
- viestintämarkkinalain yleisesti kaiken viestinnän turvallisuuteen sovellettavat yleiset periaatteet
- työelämän tietosuojalain tietoturvaluusvelvoitteiden ja sähköisen viestinnän avaamiseen liittyvät säännökset
- laki kansainvälisistä tietoturvaluusvelvoitteista
- laki turvallisuusselvityksistä
- laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista

Tietoturvaluuslaki ei kuitenkaan olisi pelkkä kodifikaatio vaan sisältäisi verkkoyhteiskunnan turvallisuuden kannalta uutta sisältöä ja ajattelua.

Yksityisen ja julkisen sektorin väliset informaatiovirrat ovat tavanomaisia ja julkisia tehtäviä tai niihin liittyviä tietojenkäsittelytehtäviä hoitavat usein yksityiset yritykset. Tietojenkäsittelyn ja järjestelmäratkaisujen osittainen tai kokonaisvaltainen ulkoistaminen on arkipäivää yksityisellä ja julkisella sektorilla. Ulkoistamiseen liittyviä vastuita ja niiden jakoa on tietoturvaluuslain sääntelyssä mietittävä perinteisiä ulkoistamisen oikeuskysymyksiä laajemmin. Lähtökohtana tulee olla ulkoistajan infrastruktuurivastuu siitä verkosta, johon kytkeytyy ja tiedon elinkaareen liittyvien oikeudellisten kysymysten ja niiden osana tietoturvaluuskysymysten asianmukaisesta hoitamisesta. Verkkoyhteiskunnan informaatiohallinto ja informaatiohallinto eivät tunne perinteisellä tavalla yksityisen ja julkisen välistä rajaa.

Tietoturvaluuslain paikka on näin osana informaatio-oikeudellista yleislainsäädäntöä ja lain soveltamisalan tulisi kattaa niin julkinen kuin yksityinen sektori. Yksityisellä sektorilla lain tulisi tarpeettomien hallinnollisten kustannusten välttämiseksi olla toissijainen eli lailla ja sopimuksella syrjäytettävä yleislaki. Tietoturvaluuslain tärkeänä tehtävänä olisi vähentää tietoturvaluudesta sopimiseen liittyviä transaktiokustannuksia, vähentää tietoturvaluusriskeihin liittyvää oikeudellista epävarmuutta ja niiden aiheuttamia kustannuksia sekä antaa työvälineitä ja pelisääntöjä tietoturvaluusvalvonnalle.

Tietoturvallisuudelle tarvitaan uusi, monia eri ohjausvälineitä käyttävä ja lakiin perustuva ohjausmalli

Tietoturvallisuus on laaja-alainen ilmiö. Sitä ei voida pakottaa vain juridiikan kaa-
puun. Tietoturvallisuus on huomattavassa määrin tietotekninen ja tietojoh-
tamiseen sekä yleensä johtamiseen liittyvä asia. Oleellista tietoturvallisuuslaissa olisikin elävän ja
kehittyvän, monitieteisen ja monimuotoisen ja mahdollisimman vaikuttavan ohjaus-
mallin luominen. Laki ja asetus sekä niitä täydentävät määräykset eivät ole riittävän
ketteriä ja tarvittavan teknisiä ohjauskeinoja.

Tietoturvallisuuslain sisältöön voisi kuulu muun muassa seuraavia elementtejä tai
asiakokonaisuuksia

1. Tietoturvallisuuden yleinen oikeudellinen määritelmä ja keskeiset tietoturval-
lisuuden kriteerit
2. Tietoturvallisuuden ja tietoturvaluustyön yleisistä periaatteista
 - o suhteellisuus riskien ja kustannusten perusteella
 - o mahdollisuus arvioida ja luottaa tietoturvallisuuden tasoon eli infor-
mointivelvoite ja avoimuusperiaate
3. Yleinen tietoturvallisuusvelvoite käsiteltäessä toisen oikeuksien kannalta
oleellista tietoa
4. Yleinen tietoturvallisuusvelvoite viestinnässä ja käytettäessä viestintään käy-
tettäviä tai siihen kykeneviä laitteita
5. Tietoturvallisuus osana sopimuksen mukaisen toiminnan ja sopimuslojalitee-
tin velvollisuuksia
6. Tietoturvallisuusjärjestelyt ulkoistettaessa toisen oikeuksien kannalta merkit-
tävää tietojenkäsittelyä
7. Oikeus käyttää tietoturvallisuusratkaisuja omien oikeuksien suojaamisessa;
purkamisen ja kieltämisen kieltö
8. Tietoturvallisuusjärjestelyiden purkamien ja avaaminen käyttäjän tai toisen
oikeuksien suojaamiseksi
9. Tietoturvallisuuden toteuttaminen hyvän tietojoh-
tamisen ja tiedonhallintata-
van avulla
10. Tunnistamisesta itsemääräämisoikeutta käytettäessä – oikeudesta turvalliseen
identiteettiin
11. Tunnistuspalveluiden markkinoinnista ja tunnistuspalvelumarkkinoista
12. Tietoturvallisuuden ohjausmalli: asetukset, käytännösäännöt ja standardit,
mallisopimukset, eräiltä osin velvoittavat määräykset
13. Tietoturvallisuus- ja henkilöturvallisuussertifioinneista ja niissä noudatettavis-
ta menettelyistä ja sertifikaattien tunnustamisesta
14. Tietoturvallisuusviranomaisesta ja sen suhteesta tietosuojavaltuutettuun. Kan-
sallisen tieto- ja verkkoturvallisuusviranomaisen toiminnan saattaminen riittä-
väälle säädöspohjalle
15. Tietoturvallisuusominaisuuksista informoinnista tuoteturvallisuuslainsäädän-
nön ja kauppalaian tapaan – toissijainen yleislaki
16. Oikeustoimien tekemisen ja todentamisen välineiden ja oikeudellisen viestin-
nän tietoturvallisuudesta
17. Riskinjaosta viestinnässä ja erilaisten verkkojen tilanteissa – esim avoimen
langattoman lähiverkon rakentaminen ja ylläpito – ei enää yksin viestintä-
markkinoiden regulaation asia
18. Tietojärjestelmien ja eri viestintäverkkojen ylläpitäjien oikeuksista
19. Toimivaltuuksista ja toimintatavoissa eräissä loukkaustilanteissa – verkosta ir-
rottamisen tai verkkoon pääsyn estämisen oikeus
20. Tietojärjestelmä- ja turvallisuusauditoinneista
21. Yhteentoimivuusvelvoitteista kilpailuoikeutta täydentävänä asiana ja rajapin-
tojen standardoinnista sekä mahdollisuudesta asettaa rajapintavaatimuksia ja
yhteentoimivuusvaatimuksia

22. Julkisten yhteiskäyttöisten tietovarantojen erityisistä yleisistä turvallisuusvaatimuksista ja turvallisuusmenettelyistä

Lopuksi

Tietoturvallisuuslain säätämiseksi voidaan alustavassa arvioinnissa esittää hyviä taloustieteeseen ja paremman sääntelyn periaatteiden toteuttamiseen liittyviä argumentteja. Asiaa tulisikin avoimesti ja ennakkoluulottomasti selvittää ja arvioida. Yhden tietoturvallisuuslain sijasta voidaan ajatella tietoturvallisuuden kokoamista muutamaankin yleislakiin. Mutta toisaalta onhan meillä vesilaki ja maankäyttö- ja rakennuslakikin. Miksi ei sitten tietoturvallisuuslaki. Ajatus on vanha ruotsalainen kaarimalli; tarvitsemme tietoturvallisuuskäynnin (informationsäkerhetsbalken)

Paremmun sääntelyn ja ohjauksen tuloksellisuuden sekä hallinnollisen taakan vähentämisen näkökulmasta olisi arvioitava kriittisesti myös nykyisiä julkisen hallinnon ohjaukselimiä ja niiden antamaa ohjeistusta. Toimijoita on liikaa eivätkä ohjeet ole informaation ja tiedon ekonomian näkökulmalla pilattuja.

Tietoturvallisuus ei toki ole vain juridinen asia. Tietoturvallisuuteen ei sovi kaavamaisesti ajatus, että lailla on maata rakennettava. Tietoturvallisuus ei tule yksin pykälillä kuntoon. Juridiikan tulee kuitenkin antaa selkeä viitekehys ja perusta tekniikan ja johtamisen ammattilaisten työlle sekä jokaisen käyttäjän ja toimijan kansalais- ja yhteiskuntavastuulle. Tietoturvallisuuslaille on viime kädessä ja painavimpana perusoikeusperustelu. Oikeus turvalliseen identiteettiin ja yleensä tietoturvallisuus ovat eurooppalaisen ihmisoikeuskehityksen valossa perusoikeuksia ja ne täytyy riittävän kattavasti ja yleisesti turvata.

Tietoturvallisuudessa on kyse ihmisestä, ihmisen oikeuksista.