Jari Råman

Yleislaki, yleiset opit ja vaikutusten arviointi – ehdotuksia tietoturvallisuuden sääntelyn kehittämiseksi

JOHDANTO

Tietoturvallisuuden sääntelyyn on kansainvälisesti herätty vauhdilla. Siinä missä 90-luvun alussa painopiste oli vielä vahvasti tietotekniikkarikosoikeudessa, on tietoturvallisuuden erillinen sääntely vuosikymmenen lopulla ollut jo vahvaa. Kun Lapin yliopiston oikeusinformatiikan instituutti vuosikymmen sitten selvitti valtiovarainministeriön pyynnöstä tietoturvallisuuden sääntelyn tilaa kansainvälisesti, yllättyivät laatijat vireillä olevien hankkeiden jatkuvasti kasvavasta määrästä ja niiden nopeasta etenemisestä.[1] Tietojenkäsittelyn toimivuuden merkitykseen koko yhteiskunnalle oli herätty, ja sen turvallisuuden sääntely on kansainvälisesti otettu kehittyneissä länsimaissa vakavasti. Työryhmä tunnistikin, eritoten kansainvälisten säädösten analyysin perusteella, tietoturvallisuuden oikeusperiaatteen olevan merkittävässä osassa oikeuksien toteuttamisessa ja turvaamisessa.

Sittemmin tahti on vain kiihtynyt. Pelkästään sääntelyllisesti keskeisillä henkilötietojen käsittelyn ja julkishallinnon tietojärjestelmien alueella sekä finanssisektorilla kehitys on ollut huimaa. Kommentaarit ovat vanhentuneet ennen kuin niitä on kirjoitettukaan. Selkeänä katalyyttinä on ollut tietoturvaloukkausten määrän ja aiheutuneiden menetysten huima kasvu. Eikä tietoturvaan kohdistuvien loukkausten saama julkisuus ja sääntelyvaatimuksia herättävä luonne näytä hellittävän. Kansainvälisessäkin katsannossa lainsäätäjät ovat länsimaissa selkeästi havahtuneet tietojenkäsittelyn toimivuuden yhteiskunnalliseen merkitykseen ja ottaneet sen turvallisuuden sääntelyn vakavasti.[2] Tie-

[1] *Ahti Saarenpää – Tuomas Pöysti* (toim.): Tietoturvallisuus ja laki: Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä, Helsinki 1997, s. 570.

[2] *Lauri Railas* tarjoaa tuoreen käytännön toimijoiden tarpeisiin vastaamaan tehdyn lyhyen yleiskatsauksen keskeisten säännösten sisältöön Pohjoismaiden lisäksi niin Saksassa, Venäjäl-

toturvallisuus koko oikeusjärjestelmän kattavana oikeusperiaatteena on tullut näin vahvasti ilmaistuksi varsin monessa maassa.

Vaikka tietoturvallisuuden sääntelyn kehitys noudattaakin pitkälti kansainvälistä linjaa, on meillä monista maista poiketen erityisesti korostettu tietoturvallisuuden roolia perusoikeuksien suojaamisessa. Sääntelyn kehitys on Suomessa kytkeytynyt ainutlaatuisella tavalla perusoikeuksiin ja niihin liittyvään lakisääteisyyden vaatimukseen. Vaikka kansallinen perusoikeuksien merkityksen korostuminen ja oikeusvaltion nousu ovat osa laajempaa perustuslaillista kehitystä yhä useammassa oikeusjärjestelmässä, on Suomessa nimenomaan lakisääteisyyden vaatimus ollut leimaa-antava piirre myös tietoturvallisuudesta säädettäessä.[3] Aiemmin pitkälti alemmanasteisen sääntelyn varassa ollut tietoturvallisuuden järjestäminen on noussut eduskuntalain tasolle.

VELVOITE EDUSKUNTALAIN KÄYTTÖÖN

Eduskuntalain tasoisen sääntelyn käytön edellyttäminen myös tietoturvallisuuden osalta on selkeässä yhteydessä *Ahti Saarenpään* esiin tuomaan muutokseen kohden oikeudellista verkkoyhteiskuntaa.[4] Tietoturvan sääntely nousee välttämättä eduskuntalain tasolle. Emme voi välttää sääntelemästä yhä monimutkaistuvaa yhteiskuntaa demokraattisessa oikeusvaltiossa.[5] Näin

---

lä kuin Virossakin liikenne- ja viestintäministeriölle laatimassaan raportissa Tietoturvallisuuslainsäädäntö: Kansainvälinen vertailututkimus, LUOTI-julkaisuja 4/2006, Helsinki 2006.

[3] Euroopan yhteisön oikeudessa laillisuusperiaate ja oikeusvaltiollisuus myös ilmenevät sääntelykeinoja valittaessa. Myös Euroopan unioni on varsin pitkälle sidottu oikeudelliseen ohjaukseen valitessaan keinoja tavoitteidensa toteuttamiseen, kuten *Tuomas Pöysti* (Tehokkuus, informaatio ja eurooppalainen oikeusalue, Helsinki 1999, s. 203) on tuonut esiin analysoidessaan yhteisön oikeuden tehokkaan vaikutuksen periaatteen lakisidonnaisuutta. Euroopan unioni ei kuitenkaan ole niin tiukasti sidottu kirjoitetun lain käyttöön johtuen yhteisön oikeuden periaatehakuisuudesta ja yhteisöjen tuomioistuimen keskeisestä roolista oikeuden kehityksessä. Ibid. s. 206–207.

[4] Muutosta kohden oikeudellista verkkoyhteiskuntaa, jossa oikeuksiemme käyttö on merkittävässä määrin siirtynyt verkkoihin ja jossa oikeudellinen viestintä on verkkopohjaista, *Saarenpää* on kuvannut useaan otteeseen. Esim. Oikeusvaltio ja verkkoyhteiskunta, teoksessa *Aulis Aarnio – Timo Uusitupa* (toim.): Oikeusvaltio, Helsinki 2002, s. 106–130, sekä E-government and Good Government: An Impossible Equation in the Network Society?, s. 246–250, in Peter Wahlgren (ed.): IT Law, Scandinavian Studies in Law, Vol. 47, Stockholm 2004, s. 245–275.

[5] *Saarenpää*: E-government and Good Government, s. 249.

välttämättä onkin. Monimutkaistuvassa yhteiskunnassa tarvitsemme yhä enemmän suojaa oikeuksillemme.

Autonomian ajan loppukauden sortovuosilta (1899–1905) periytyvän vahvan legalismin[6] ohella lähtökohtana ovat tietoturvallisuuden moninaiset perusoikeuskytkennät. Tietoturvallisuus on jo pitkään selkeästi hahmotettu perusoikeuksiemme ja -vapauksiemme käytön välttämättömäksi edellytykseksi informaatioyhteiskunnassa. Kyse on niin yhteiskunnan toimivuuden kuin myös yksilön oikeuksien toteutumisen takeesta. Jo tässä muodossa, niin sanottuna kollektiivisena hyvänä toimivana yhteiskunnallisena tavoitetilana, se edellyttää lainsäätäjältä aktiivisia toimenpiteitä.[7] Tietoturvallisuuden hahmottaminen myös yksilön henkiseen koskemattomuuteen ja tiedolliseen itsemääräämisoikeuteen liittyväksi oikeudeksi tuo lakisääteisyyden vaatimuksen entistä selkeämmin näkyviin.[8]

> Suomalaisessa tietoturvallisuuden oikeudellisessa keskustelussa tietoturvallisuus on nähty ensisijaisesti metaperusoikeutena. Tietoturvallisuus on tällöin, kollektiivisena hyvänä, viestintäjärjestelmien häiriöttömän toiminnan ja koko informaatioinfrastruktuurin toimivuuden edellytys, sekä perusoikeuksien turvallisen käytön mahdollistaja tietoverkoissa. Tietoturvallisuus on yksi perusoikeusjärjestelmämme tavoitteista ja perusoikeuksien toteutumisen edellytyksistä. Tämä jo vuoden 1997 selvityksessä esiin tuotu ajatus on saanut rinnalleen tulkinnan tietoturvallisuudesta yksilöllisenä oikeutena.

---

[6] *Jaakko Nousiainen*: Suomen hallitusjärjestelmä: Sekoittuneesta valtiomuodosta parlamentaariseen, Oikeusministeriö, otsikko "Historiallinen ja yhteiskunnallinen tausta", 4. kappale, osoitteessa http://www.om.fi/Etusivu/Perussaannoksia/Perustuslaki/Yhteiskunnallinenjahistoriallinentausta [päivitetty 9.2.2000, vierailtu 9.10.2006].

[7] Tätä on erityisesti *Ahti Saarenpää* pitänyt oikeusinformatiikan tutkimuksessa esillä. Esim. *Saarenpää*: Oikeusvaltio ja verkkoyhteiskunta, s. 119. Lailla säätämisen vaatimus tulee esiin erityisesti tilanteissa joissa tietoturvallisuus on perusoikeuksien kanssa kollisioissa oleva hyväksyttävä rajoitusperuste. Haastavin esimerkki lienee sähköisen viestinnän tietosuojalain (516/2004) 20 § tietoturvan toteuttamiseksi välttämättömien toimenpiteiden sallimisesta. Varsin monikerroksisessa pykälässä rajoitetaan niin perusoikeuksiamme viestinnän luottamuksellisuuteen, yksityisyyteen, sananvapauteen kuin tietoturvallisuuteenkin, kollektiivisena tavoitetilana olevan tietoturvallisuuden toteuttamiseksi ja sähköisen viestinnän toimivuuden takaamiseksi. Perusoikeudet on laajasti huomioitu säännöksen perusteluissa (HE 125/2003 vp, yksityiskohtaiset perustelut). Myös perustuslakivaliokunta käsitteli säädöstä laveasti lausunnossaan PeVL 9/2004 vp. Lailla säätämisen vaatimusta osana perusoikeuksien yleisiä rajoitusedellytyksiä esittelee erityisesti V*eli-Pekka Viljanen* väitöskirjassaan Perusoikeuksien rajoitusedellytykset, Helsinki, 2001, s. 65–115.

[8] Perustuslakimme 80 §:n 1 momentin ilmaiseman periaatteen mukaan yksilön oikeuksien ja velvollisuuksien perusteista on säädettävä lailla.

> *Ahti Saarenpään* kanssa suomalaisen tietoturvallisuuden oikeudellisen tutkimuksen kantavan voiman muodostava *Tuomas Pöysti* oli vielä uuden vuosituhannen taitteessa empien sitä mieltä, ettei tietoturvallisuus välttämättä olekaan yksilöllinen oikeus.[9] Myös Ahti Saarenpää on korostanut lähinnä tietoturvallisuuden metaperusoikeusluonnetta.[10] Vuonna 2004 tietoturvallisuus liitettiin selkeämmin osaksi perustuslaissa suojattua henkilökohtaiseen vapauteen ja koskemattomuuteen kiinteästi liittyvää oikeutta turvallisuuteen (PL 7.1 §) ja yksityiselämän suojaan kytkeytyvää oikeuttamme identiteettiin (PL 10 §).[11]

Tietoturvallisuudesta on näin lähtökohtaisesti säädettävä lailla. On sitten kyse tilanteesta, jossa tietoturvallisuus esiintyy perusoikeuksien kanssa kollisiossa olevana hyväksyttävänä rajoitusperusteena tai yksilöllisenä oikeutena, jonka perusteista on säädettävä lailla.

LAKISIDONNAISUUDEN ONGELMIA

Tietoturvallisuuden selkeä kytkentä perusoikeuksiin ja sääntelyn nouseminen eduskuntalakien tasolle on ehdottomasti positiivinen kehityssuunta. Verk-

---

[9] *Tuomas Pöysti*: Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin turvallisuutta, s. 96–99, Oikeus 2000:1, s. 91–112.

[10] Ks. mm. *Ahti Saarenpää*: Verkkoyhteiskunnan oikeutta – johdatusta aiheeseen, s. 14, Oikeus 2000:1, s. 3–15; *sama*: Näkökohtia tietoturvallisuudesta ja sen sääntelystä verkkoyhteiskunnassa, s. 104–106, Pohjoissuomen tuomarikoulun julkaisuja 4/2001, Rovaniemi 2002, s. 75–109; *sama*: Data Security: A Fundamental Right in the e-Society?, p. 424–429, in Klaus Lenk and Roland Traunmüller (eds.) Electronic Government: First International Conference, EGOV 2002, Aix-en-Provence, France, September 2-5, 2002, Proceedings. Lecture Notes in Computer Science 2456, Springer 2002; ja vielä vuonna 2005 *sama*: Tietojenkäsittelystä läsnä-älyyn – katkelmia oikeusinformatiikan kehityksestä, s. 110, teoksessa Juha Tolonen – Vesa Annola – Brita Herler (toim.): Talousoikeuden taitekohtia. Juhlajulkaisu professori Asko Lehtoselle, Vaasa 2005, s. 91–123. Metaperusoikeus näkökulma on tuotu ensimmäisen kerran esiin, Tuomas Pöystin aloitteesta, jo mainitussa valtiovarainministeriölle laaditussa raportissa (*Saarenpää*: E-government and Good Government, s. 261 alaviite 51).

[11] *Tuomas Pöysti*: ICT and Legal Principles: Sources and Paradigm of Information Law, s. 590, in Peter Wahlgren (ed.) IT Law, Scandinavian studies in law 47, Stockholm Institute for Scandinavian Law, Stockholm 2004, s. 559–601. *Saarenpää* (E-government and Good Government, s. 260) kyllä puhuu yksilöllisestä oikeudesta tietoturvallisuuteen samassa juhlakirjassa, mutta ei nosta sitä vielä perusoikeuden tasolle. Sen sijaan hän tyytyy tarkastelemaan tietoturvallisuuden määrittämistä yksilölliseksi oikeudeksi vain yhtenä lakiteknisenä ratkaisuna alan sääntelyssä.

koyhteiskunnassa myös tietoturvallisuus oikeudellistuu. Perusoikeuksiemme suoja tietoverkkojen aikakaudelle vaatii sitä. Näin tietoturvallisuuden merkitys tulee yksiselitteisesti esiin. Tästä huolimatta tiukan perusoikeussidonnainen tietoturvallisuuden sääntely voi olla myös vaarallinen kehityssuunta. Se nimittäin laajentaa eduskuntalain tasoista sääntelyä edellyttävien tilanteiden määrää merkittävästi.

Näin erityisesti silloin, kun perusoikeuksien suoja horisontaalisissa yksityisten toimijoiden välisissä suhteissa otetaan vakavasti, kuten tietoturvallisuuden osalta tulisi tehdä. Yksityisten toimijoiden, kuten informaatioinfrastruktuurin ylläpitäjien ja sähköisen viestinnän palvelun tarjoajien, mahdollisuudet puuttua yksilöiden perusoikeuksiin kasvavat verkkoyhteiskunnassa.

Tilanteessa, jossa yksilön ja hänelle palveluja järjestävän tahon välillä on selkeä erivertaisuus ja jossa vahvemman vallan käyttö saattaisi ilman selkeästi asetettuja sääntöjä uhata yksilöiden perusoikeuksien toteutumista, on selkeänä lähtökohtana oltava yksilön perusoikeuksien suojaaminen myös muualta kuin valtiovallan taholta tulevilta loukkauksilta. Yksilö on näihin yksityisiin toimijoihin nähden niin eriarvoisessa asemassa, että hänen oikeutensa tarvitsevat erityistä suojaa – aivan samalla tavalla kuin julkisen vallankin toimia vastaan. Pitäytyminen pelkästään siinä liberaalille oikeusvaltiolle ominaisessa käsityksessä vapausoikeusluonteisista perus- ja ihmisoikeuksista, jonka mukaan näiden oikeuksien ensisijainen vaikutusalue on julkisen vallan ja yksityisen välisessä vertikaalisuhteessa, voisi verkkoyhteiskunnassa osoittautua kohtalokkaaksi yksilön oikeuksien kannalta.[12]

Tämä tulee selkeästi esiin Lex Soneraksi kutsutusta sähköisen viestinnän tietosuojalaista (516/2004).[13] Laki ja sen taustalla oleva direktii-

---

[12] Perusoikeutena turvallisuuden itsenäinen merkitys yleisesti ja tietoturvallisuuden merkitys erityisesti tulee esiin nimenomaan horisontaalisuhteissa. Vaikka turvallisuus yksilöllisenä perusoikeutena ei juurikaan omaisi sellaista itsenäistä sisällöllistä merkitystä valtion ja kansalaisten välisessä vertikaalisuhteessa, joita jo itsemääräämisoikeutta monipuolisesti turvaavat oikeudet vapauteen, koskemattomuuteen ja yksityisyyteen eivät kattaisi, on sillä kuitenkin itsenäistä merkitystä korostaessaan nimenomaan julkisen vallan aktiivista toimintavelvoitetta henkilökohtaisen turvallisuuden osalta sekä ulottaessaan turvallisuuden perusoikeutena yksityisten välisiin horisontaalisuhteisiin. Julkisen vallan aktiivisen toimintavelvoitteen korostaminen on ollut jo hallituksen perusoikeusesityksen tarkoitus, kuten *Viljanen*: Perusoikeuksien rajoitusedellytykset, s. 165–168, osoittaa.

[13] Lisänimi tulee tunnistamistietojen käsittelyä koskevien lokitietojen, eli tapahtumatietojen siitä kuka tunnistetietoja on käsitellyt, milloin ja kuinka kauan, tallentamisvelvollisuuden nostamisesta eduskuntalain tasolle Sonerassa ilmenneiden väärinkäytösten myötä. Tapaus ei enää ole mitenkään ainutlaatuinen, kuten jo kohu laittomien toimintamenetelmien käytöstä laite- ja palvelutoimittaja Hewlett-Packardin hallituksen sisäpiirivuotojen tutkimuk-

vi[14] ovat osoituksia julkisen vallan velvollisuuksista huolehtia erilaisten perusoikeuksien toteutumisesta perusinfrastruktuurin sääntelyssä. Lähes jokaiseen lain säännökseen liittyy lähemmässä tarkastelussa merkittäviä perusoikeuskytkentöjä. Lain tavoitteena on sähköisen viestinnän käyttäjien oikeuksien toteutumisen turvaaminen muualta kuin valtion taholta, siis ennen kaikkea muilta yksilöiltä ja yhteisöiltä tulevia loukkauksia vastaan. Laki keskittyy yksityisten toimijoiden, ennen kaikkea teleyritysten, heiltä viestintäpalveluja tilaavien yhteisöjen ja yksityisten välisten suhteiden sääntelyyn, kun taas viestintämarkkinalaki on leimallisesti alan toimijoiden suhteita järjestävä laki.[15]

Positiivisen perusvireen rinnalle tietoturvallisuuden eduskuntalaintasoisessa sääntelyssä on säädösten kasvavan määrän lisäksi noussut huoli sääntelyn laadusta ja hajanaisuudesta. Uhkana ovat jo osittain näkyvissä olevat tulkintakäytäntöjen hajaantuminen ja alakohtaisten lakien eriytyminen tilanteessa, jossa tietoturvallisuuden ongelmat esiintyvät suhteellisen samanlaisina ja edellyttäisivät varsin samanlaisia sääntelyllisiä ratkaisuja. Nyt kansainvälisestikin valitulla tietoturvallisuuden alakohtaisella erityissääntelyn linjalla tiukka lakisääteisyyden vaatimus yhdistettynä vahvan legalistiseen sääntelykulttuuriimme johtaa helposti varsin yksityiskohtaisiin ja jäykkiin eduskuntalain tasoisiin säännöksiin keskeisesti dynaamisuutta edellyttävän ilmiön sääntelyssä.[16] Sa-

---

sessa osoittaa. Ks. esimerkiksi uutisointia Tietoviikosta, *Juho Pentikäinen*: Syytteet kolahtivat Dunnille ja neljälle muulle, 5.10.2006, 08:34, osoitteessa http://www.tietoviikko.fi/ [11.10.2006].

[14] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi), Virallinen lehti nro L 201, 31.7.2002, s. 37–47.

[15] Sähköisen viestinnän tietosuojalain rooli yksityisten toimijoiden välisten suhteiden sääntelyssä tulee selkeästi esiin myös perustuslakivaliokunnan lausunnosta PeVL 9/2004 vp (valiokunnan kannanottojen perustelujen yleinen osuus). Olemme analysoineet perusoikeuksien huomioonottamista sähköisen viestinnän tietosuojalain yhteydessä liikenne- ja viestintäministeriölle laatimassamme kansallisen tietoturvallisuusstrategian täytäntöönpanoon liittyvässä raportissa. *Ahti Saarenpää – Rauno Korhonen – Jari Råman*: Sähköinen viestintä, tietoturvallisuus ja perusoikeudet, Lapin yliopiston oikeusinformatiikan instituutin raportti liikenne- ja viestintäministeriölle, 2004, julkaistu kansallisen tietoturvallisuusstrategian toimeenpanoa tukevan kansallisen tietoturvallisuusasioiden neuvottelukunnan toimintasuunnitelman kohdan 4.1 ”Perusoikeuksien huomioonottaminen” osana. Raporttiin löytyy linkki liikenne- ja viestintäministeriön sivuilta kohdasta Viestintätietoa – Tietoturva ja tietosuoja – Kansallinen tietoturvastrategia.

[16] Sääntelyn kehittämisen kannalta kritiikkiä legalistinen sääntelykulttuurimme ja uuden perustuslain mukanaan tuoma laajentunut lakisääteisyyden vaatimus ovat saaneet osakseen erityisesti OECD:n Suomea koskeneessa raportissa, OECD, Government Capacity to As-

malla nykyisen sääntelylinjan ongelmat hajanaisuudesta ja säännösten suuresta määrästä vain kasvaisivat.[17]

Huolena on erityisesti yksi demokraattisen oikeusvaltion kulmakivistä – kansalaisten velvollisuus tuntea laki. Sinällään jo huoli tästä idealistisesta oletuksesta, jota uhkaa muutos utopiaksi, on vakava. Viime kädessä kyse on lainkäyttäjän legitimiteetistä ja oikeuden uskottavuudesta.

Samalla huolena on aidosti myös sääntelyn vaikuttavuus. Mikäli sääntelyn kohteet eivät tunne lakia, ei lain tavoitteita tulla saavuttamaan.[18] Sääntelyn sirpaloitumisesta johtuen jo soveltuvan lainsäädännön tunnistaminen ja omaan toimintaan kohdistuvien oikeudellisten velvoitteiden löytäminen vaatii ammattitaitoa. Säännösten nopea muutostahti ja yhteneväisyyden puute ei missään nimessä helpota lain asettamia velvoitteita noudattamaan pyrkivien toimintaa.[19] Näin erityisesti siksi, että sääntelyn ensisijainen lukijakunta ja pääasialliset soveltajat – tietoturvavastaavat – eivät ole saaneet oikeustieteellistä koulutusta.

Uhkana on samalla myös perusoikeuksien toteutumisen vaarantuminen sirpaloituneen ja tulkinnaltaan hajanaisen lainsäädännön vuoksi. Uhkana on

---

sure High Quality Regulation in Finland, OECD Reviews of Regulatory Reform, Paris 2003, saatavilla osoitteessa http://www.oecd.org/ [2.10.2006].

[17] Huoli tietoturvallisuuden sääntelyn hajanaisuudesta ja yhtenäisen linjan puutteesta ei sinällään ole mikään uusi. Pohjoismaisessa oikeusinformatiikan tutkimuksessa hajanaisuuden aiheuttama ongelma on ollut mukana heti alusta alkaen. *Peter Seipel* nosti esiin tietoturvallisuuden sääntelyn hajanaisuuden vuonna 1977 julkaistussa ensimmäisessä oikeusinformatiikan alaan liittyvässä väitöskirjassa Computing Law: Perspectives on a New Legal Discipline, LiberFörlag, Stockholm 1977, s. 83–87. Tietoturvallisuuden sääntelyä on jo pitkään tuotettu eri aloilla vailla selkeää yhtenäistä linjaa. Ratkaistavana olevia sääntelyongelmia on perinteisesti tarkasteltu pelkästään kyseisen alan tai käsiteltävän informaation spesifisistä lähtökohdista ja omin käsittein ilman yhteyttä vastaaviin tilanteisiin laajemmin. Tällä hetkellä yritysten ja yhteisöjen oikeudelliset tietoturvallisuusvelvoitteet asetetaan yhä laajenevassa joukossa lähtökohdiltaan ja sisällöltään vaihtelevia alakohtaisia lakeja, alemman asteisia säännöksiä, sekä yksityisoikeuden doktriineja ja oikeustapauksia.

[18] Tämä ei merkitse sitoutumista rationaalisen päätöksenteon malliin. Epätäydellinenkin informaatio saa aikaan vaikutuksia, eivätkä kaikki ole vastaanottavaisia täydellisellekään informaatiolle. Toisaalta sääntelytieto voi vaikuttaa käyttäytymiseen myös tiedostamatta erilaisten osittain tuntemattomien välittävien mekanismien kautta.

[19] Toimintaympäristön jatkuva kehittyminen saa aikaan toistuvan tarpeen muuttaa jo olemassa olevia säännöksiä. Sähköisen viestinnän tietosuojalaki on yksi ääriesimerkeistä. Se on ollut jatkuvassa muutoksessa vuodesta 1999, kun lain ensimmäinen versio säädettiin. Nykyistä sähköisen viestinnän tietosuojalakia (516/2004) edelsi laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999), jota ennätettiin muuttaa kuusi kertaa ennen kumoamistaan nykyisellä lailla vuonna 2004. Nykyistäkin lakia on ennätetty jo muuttaa kaksi kertaa ja uusia muutoksia valmistellaan parasta aikaa.

se, että eduskunta tuottaa niin paljon erisuuntaisia yhteiskuntapoliittista merkitystä omaavia säännöksiä, että tietoturvallisuutta koskeva lainsäädäntö yleensä ei saavuta sille asetettuja yhteiskunnallisia tavoitteita turvallisemmasta informaatioinfrastruktuurista ja luottamuksesta sähköisiin palveluihin ja markkinoihin.[20] Kyse ei ole yksittäisen säännöksen tavoitteista, vaan koko tietoturvallisuutta koskevan oikeudellisen sääntelykehyksen tavoitteiden saavuttamatta jäämisestä.

Oikeudellistumisen ongelmat eivät ole uusia verkkoyhteiskunnassa, eivätkä sinällään ratkaisuehdotuksetkaan. Samat teemat ovat olleet esillä jo 1980-luvulta alkaneessa sääntelyn vähentämiseen pyrkivien hankkeiden aallossa.[21] Tässä yhteydessä on kuitenkin syytä tarkastella tietoturvallisuuden sääntelyn kehityksen kannalta kahden keskeisen ratkaisuehdotuksen, säädösten tulkinnan yhtenäistämisen ja niiden systematisoinnin, haasteiden erityispiirteitä.

OIKEUSTIETEEN ROOLI

Kuten *Kaarlo Tuori* on kriittisen oikeuspositivismin ohjelmassaan oikein korostanut, päävastuu oikeuden sisäisen rationaalisuuden vaalimisesta on lainkäytössä ja oikeustieteessä, ei lainsäätämismenettelyssä. Lainsäätäminen poliittis-oikeudellisena käytäntönä tuottaa yksittäisiä säädöksiä, jotka on vielä tulkittava ja saatettava toistensa kanssa systemaattisiin yhteyksiin, ennen kuin oikeus voi toteuttaa yhteiskunnalliset tehtävänsä. Tulkinnasta ja systematisoinnista vastaavat ensisijaisesti oikeudenkäyttö ja oikeustiede.[22]

---

[20] *Ilkka Saraviita* esitti vuonna 2000 huolensa eduskuntakäsittelyn jäämisestä pelkäksi muodollisuudeksi, mikäli asetuksenantovallan rajaukset lisäävät merkittävästi eduskunnan työmäärää ja tuovat eduskuntaan runsaasti sellaista teknisluonteista lainsäädäntöä, jolle ei ole yhteiskuntapoliittista merkitystä (Perustuslaki 2000: Kommentaariteos uudesta valtiosäännöstä Suomelle, Helsinki 2000, s. 386). Eduskunnan työmäärä myös tietoturvallisuutta koskevan lainsäädännön käsittelyssä on selkeästi noussut, mutta muodollisuudeksi eduskuntakäsittely ei ole jäänyt. Yksityiskohtaisesta lainsäädännöstä huolimatta tietoturvallisuuden sääntely on koskenut merkittäviä perusoikeuksiin liittyviä yhteiskuntapoliittisia kysymyksiä.

[21] Lainsäädäntötutkimuksessa *Jyrki Tala* arvioi eri oikeussääntelyn määrän vähentämishankkeita muun muassa tutkimusraportissaan 1990-luvun lopulta, Oikeussääntelyn määrä ja vaihtoehdot, Oikeuspoliittisen tutkimuslaitoksen julkaisuja 163, Helsinki 1999, s. 45–68.

[22] *Kaarlo Tuori*: Kriittinen oikeuspositivismi, Helsinki 2000, s. 153–154. *Weberiltä* lainaamallaan sisäisen rationaalisuuden käsitteellä *Tuori* viittaa lainsäädännön loogiseen konsistenssiin ja oikeusjärjestyksen sisäiseen koherenssiin. Ibid. s. 151–152.

Tietoturvallisuuden osalta tuomioistuinten mahdollisuudet tulkintakäytäntöjen yhtenäistämiseen ovat rajalliset. Tietoturvallisuutta koskevia juttuja edelleen harvoin viedään tuomioistuimeen ja silloinkin tietoturva-alan tuntemus riippuu pitkälti todistajina kuultavien asiantuntijoiden lausunnoista. Tietotekniikkarikostapausten käsittely on sinällään poikkeus ja tulkintoja on yhtenäistetty aina korkeinta oikeuttamme myöten.[23]

Lähtökohtaisesti niin tietoturvallisuuslainsäädännön tulkitsijoina kuin oikeustapausten antamien oikeusohjeiden lukijoina ovat kuitenkin oikeustieteellistä koulutusta vailla olevat tietoturvan ammattilaiset. Tuomioistuimen vahvistama oikeussäännön tavoitettavuus ja ymmärtäminen ovat tällöin pitkälti median varassa. Tietoturvallisuuteen liittyvät jutut saavat yleensä merkittävästi julkisuutta. Median kautta välittyvä viesti kuitenkin helposti vääristyy.

Yksi yhä enenevässä määrin käytetty ratkaisukeino on oikeuden ammattilaisten roolin kasvattaminen tietoturvallisuudesta huolehtimisessa ja laajemmin tietoon kohdistuvien riskien hallinnassa. Tarve eri ammattiryhmien välisen keskustelun lisäämiselle on ilmeinen. Tällöin tietoturvan ammattilaisten tarve osata löytää, tunnistaa ja tulkita soveltuva laki tai muuten asetettu oikeussääntö vähenee. Riittää, että heillä on kyky tunnistaa mahdolliset oikeudellisia ongelmia nostattavat tilanteet ja kääntyä oikeuden ammattilaisen puoleen riittävän aikaisin. Juristit on koulutettu tuomaan yksittäiset pykälät yhteyksiin toisten kanssa ja katsomaan sääntelyn kokonaiskuvaa.

Tämä asettaa vahvoja odotuksia juristien uudenlaiselle, ennakoivammalle ammattitaidolle. Vaikka yksittäistenkin vastuuriskien oikeudellisesti kestävä hallinta on tullut yhä vaikeammaksi, mistä selkeänä esimerkkinä ovat tietotekniikkasopimuksissa varsin laajasti käytetyt vastuuvapauslausekkeet ja niiden oikeudellisen sitovuuden ongelmat, on juristin pystyttävä samalla keskittymään riskienhallinnan kokonaiskuvaan ja tarkasteltava sitä myös liiketoiminnan näkökulmasta. Muuten riskienhallinnasta uhkaa tulla liian defensiivistä.

Erityisenä ongelmana tälle lähestymistavalle ovat asenteet. Juristien on edelleen vaikea asennoitua muuttuvaan rooliinsa riskienhallinnoijina riitojen ratkaisun sijaan.[24] Eikä oikeudellisen asiantuntemuksen tarvetta palve-

---

[23] Erityisesti on mainittava maksuvälinepetoksen tunnusmerkistön täyttymistä koskeva tapaus KKO 1999:110 sekä tietomurron yritystä koskenut porttiskannaus tapaus KKO 2003:36. Molemmissa tietoturvallisuuden rooli infrastruktuurin suojaamisessa oli korostuneesti esillä.

[24] Kyse on niin taloudellisista, työnjaollisista kuin psykologisistakin esteistä, kuten *Peter Wahlgren* kuvaa riskianalyysiä osana juristin perusmetodia tarkastelevassa teoksessaan Juridisk riskanalys: Mot en säkrare juridisk metod, Stockholm 2003, s. 139–141.

lujen ja tuotteiden kehityksessä ole vieläkään helppoa perustella. Hidasteena ovat myös tietoturvan ja oikeuden ammattilaisten mahdollisuudet tunnistaa tietoturvaan liittyvät oikeudelliset ongelmat. Jo pelkkä oikeudellisten velvoitteiden kartoittaminen on hankalaa.

Juristien perusmetodin soveltaminen, *yleisten oppien* hyödyntäminen oikeudellisen ongelman paikantamisessa, on tässä mielessä toimivampi ratkaisu. Niiden avulla laajan sääntelyinformaation hallinta helpottuisi merkittävästi ja tietoturvallisuus oikeusperiaatteena olisi selkeämmin hahmotettavissa. Osaltaan se vaikuttaisi sääntelyn tulkintojen yhdenmukaistamiseen ja voisi edistää yhdenmukaisten sääntelyratkaisujen kehittämistä. Vähintäänkin se toisi tietoturvallisuuden sääntelyn asiantuntemuksen lähemmäksi niitä lainsäätämismenettelyyn kuuluvia käytäntöjä, jotka pyrkivät varmistamaan uuden lainsäädännön sisäisen rationaalisuuden.[25] Selkeästi muotoillut tietoturvallisuuden yleiset oikeudelliset opit olisi myös suhteellisen helppo sisällyttää niin tietotekniikan ja tietojenkäsittelyn kuin oikeustieteenkin opetusohjelmiin.

Oikeustiede on monessa maassa jo reilut kymmenen vuotta pyrkinyt hahmottamaan tietoturvallisuuden yleisiä oppeja.[26] Ne eivät kuitenkaan ole vielä saaneet selkeää muotoilua ja sellaista asemaa, jonka keskeinen verkkoyhteiskunnan toimintaa koskevan ilmiön sääntely ansaitsisi. Näin siitä huolimatta, että tietoturvallisuus oikeusperiaatteena on noussut vahvasti esiin myös kansainvälisesti. Nykymuodossaan yleiset opit eivät tuo vaadittavaa systemaattisuutta tulkintojen yhtenäistämiseksi ja oikeusjärjestyksen koherenssin saavuttamiseksi. Tämä periaatteiden ja sääntelyllisten lähtökohtien jäsentymättömyys osaltaan myös selittää tietoturvallisuuden sääntelyn pirstaleisuutta.

Suomessa yleisten oppien selkeämmässä hahmottamisessa ja esiintuonnissa on viime aikoina kuitenkin otettu askelia oikeaan suuntaan. Tietotur-

---

[25] Tällaista tehtävää toteuttavat esimerkiksi ministeriöiden lainvalmistelun vahvasti edustettuina olevat oikeuden ammattilaiset, oikeusministeriön lainvalmisteluosasto, oikeuskanslerinvirasto vartioidessaan ministeriöiden lainvalmistelun ja hallituksen lakiesitysten oikeudellista moitteettomuutta sekä eduskunnan perustuslakivaliokunta oikeudellisine asiantuntijoineen. *Tuori*: Kriittinen oikeuspositivismi, s. 153.

[26] Tuoreimmat oikeustieteen pohjoismaiset pyrkimykset tietoturvallisuuden lainsäädännön edes osittain kattavaan analyysiin on tehty Norjassa. Katso erityisesti *Are Vegard Haug*: Rettslige reguleringer av informasjonssikkerhet, CompLex 2/06, Institutt for rettsinformatikk – Unipub, sekä artikkelikokoelma *Arild Jansen – Dag Wiese Schartum* (red.): Informasjonssikkerhet: Rettslige krav til sikker bruk av IKT, Bergen 2005.

vallisuuden perusoikeuslähtöisyydestä ja tietoturvallisuuden perusoikeuskytkentöjen ymmärtämisestä on enää lyhyt matka tietoturvallisuuden yleisten oppien selkeään hahmottamiseen. Perusoikeudet osoittavat varsin yksinkertaisella tavalla tietoturvallisuuden sääntelyn peruslähtökohdat. Kehitystä on viime aikoina tapahtunut erityisesti yksittäisten lainsäädäntöhankkeiden valmistelun yhteydessä suoritettujen perusoikeusanalyysien kautta. Tässä yksittäisten ministeriöiden hankkeilla on ollut keskeinen rooli.[27]

Yleisten oppien kehittyminen vaatii kuitenkin oikeustieteen entistä syvempää mukaantuloa. Tietoturvallisuuden yleisten oppien kehittämisessä on vielä paljon haastetta oikeustieteelle. Lyhyellä tähtäimellä oikeustieteen mahdollisuus vaikuttaa sääntelyn kehitykseen on vähäinen. Pidemmälläkin tähtäimellä edellytyksenä on niiden opetuksen sisällyttäminen tietoturvan ammattilaisten seuraavan sukupolven opetukseen ja nykyisen koulutukseen.

YLEISLAIN SÄÄTÄMINEN KEINONA VÄHENTÄÄ ONGELMIA

Kuten *Kaarlo Tuori* on osuvasti huomauttanut, oikeusjärjestyksen sisäisen rationaalisuuden kannalta lainsäätäminen on usein pikemminkin epäjärjestystä kuin järjestystä tuottava tekijä; oikeuden koherenssia ylläpitävät muut oikeudelliset käytännöt.[28] Yleislakien säätäminen, kodifiointi ja sääntelyn yksinkertaistaminen ovat tästä harvinainen poikkeus lainsäätämismenettelyssä. Niiden avulla oikeudellisen sääntelyn selkeyttä, ymmärrettävyyttä ja käyttökelpoisuutta voidaan parantaa lainsäätäjän toimesta.

Tietoturvallisuuden oikeudellisten periaatteiden esiintuonti henkilötietojen käsittelyn sääntelyn tehokkaaksi osoittamalla yleislakia hyödyntävällä

---

[27] Liikenne- ja viestintäministeriöllä ja erityisesti sähköisen viestinnän tietosuojalain valmistelulla muutoksineen on ollut tässä merkittävä rooli – niin positiivisessa kuin negatiivisessakin mielessä. Kuten jo yllä on huomautettu, niin hallituksen esityksessä 125/2003 vp kuin siihen liittyvässä perustuslakivaliokunnan lausunnossa PeVL 9/2004 vp, tietoturvallisuutta osana perusoikeuksia on tarkasteltu suhteellisen laajasti. Ministeriö on myös tilannut perusoikeuksien huomioonottamista tietoturvallisuuteen liittyvän sääntelyn valmistelussa tarkastelevia selvityksiä, jotka on julkaistu kansallisen tietoturvallisuusstrategian toimeenpanoa tukevan kansallisen tietoturvallisuusasioiden neuvottelukunnan toimintasuunnitelman kohdan 4.1 ”Perusoikeuksien huomioonottaminen” osana. Raportteihin löytyy linkki liikenne- ja viestintäministeriön sivuilta kohdasta Viestintätietoa – Tietoturva ja tietosuoja – Kansallinen tietoturvastrategia.

[28] *Kaarlo Tuori*: Kriittinen oikeuspositivismi, Helsinki 2000, s. 154.

tavalla voisi paremmin tuoda selkeyttä ja yhteneväisyyttä alan sääntelyyn. Samalla yleislaki osoittaisi tietoturvallisuuden yhteiskunnallisen merkityksen ja vakiinnuttaisi sen järjestämisen perusteet, loisi yhteisen sääntely- ja tulkintapohjan josta poikkeaminen erityislaeissa vaatisi perusteluja, sekä yhdistäisi julkisen ja yksityisen sektorin tietoturvan tasoa. Tietoturvallisuuden periaatteellisen merkityksen osoittaminen, perusoikeuskytkentöjen sekä tietoturvallisuuden selkeiden lähtökohtien ja yleisten periaatteiden esiintuominen yleislaissa voisi luoda tietoturvallisuuden sääntelylle kestävän pohjan.

1990-luvulla Pohjoismaissa tehtiin useampia ehdotuksia tietoturvallisuuden yleislaeiksi, mutta ne ovat johtaneet vain osittaisiin sääntelyllisiin ratkaisuihin.[29] Niin yksityiseen kuin julkiseen sektoriinkin soveltuvia yleislakeja ei tiedossani ole kansainvälisestikään. Uudella vuosituhannella suuren suosion saavuttaneet kansalliset tietoturvallisuuden strategialinjaukset erityisesti Pohjoismaissa ovat jälleen ottaneet sääntelyn kehittämisen vakavasti. Politiikkalinjauksissa sääntelyn ongelmat tunnustetaan ja tarve yhdenmukaistamiselle nostetaan esiin.[30]

Ruotsin hallitus esityksessään yhteiskunnan turvallisuudesta ja valmiudesta ilmoitti vuonna 2001 aikomuksestaan toteuttaa tietoturvallisuusasioita koskevien säännösten uudelleentarkastuksen (genomföra en översyn).[31] Ruotsin puolustusministeriön asettama selvitysmies tuo vuonna 2005 laaditussa ehdotuksessaan tietoturvallisuuspolitiikaksi kuitenkin esille, että säädösten laajamittaista uudelleenarviointia ei ole edes aloitettu. Kehitystyö on kohdistunut vain tiettyjä aloja koskeviin lainsäädännöllisiin muu-

---

[29] Norjassa yleistä tietoturvallisuuslakia esitettiin jo 1990-luvun alussa. Ehdotus ei kuitenkaan mennyt läpi. Syistä ja seurauksista ks. *Saarenpää – Pöysti*: Tietoturvallisuus ja laki, otsikko 11.8. s. 407–417 ja siinä esitetyt viitteet. Pohjoismaisia 1980- ja 1990-luvun alun lainsäädäntöaloitteita arvioidaan myös Pohjoismaiden ministerineuvoston raportissa Information Security in Nordic Countries, Nordiske Seminar- og Arbejdsrapporter 1993:613, Nordic Council of Ministers. Yleislain säätämistarve oli yksi keskeisistä ehdotuksista Oikeusinformatiikan instituutin valtiovarainministeriölle tekemässä selvityksessä tietoturvallisuuden sääntelystä vuonna 1997 (*Saarenpää – Pöysti*: Tietoturvallisuus ja laki). Ajatus on sittemmin ollut toistuvasti alan tutkimuksessa esillä.

[30] Lainsäädäntötutkimuksessa on korostettu että sääntelyn yksinkertaistamisen ja kodifioinnin tarvetta ja hyödyllisyyttä painotetaan usein erityisesti oikeusjärjestyksen ei-ammattimaisten käyttäjien kannalta. Näin esimerkiksi *Tala*: Oikeussääntelyn määrä ja vaihtoehdot, s. 58. Ehkä juuri tästä syystä yleislain tarve ja sääntelyn yhtenäisyyden kehittäminen tulevat kirjatuksi strategialinjauksiin.

[31] Regeringens propositionen av Samhällets säkerhet och beredskap, prop. 2001/02:158, otsikko 17.1. alaotsikko ”Författningsfrågor”, s. 106.

toksiin.[32] Ehdotuksessa nostetaan esille tarve luoda yhdenmukainen ja kattava sääntelykehikko tietoturvallisuudelle, mutta sen mahdollinen toteuttaminen jätetään myöhemmin analysoitavaksi. Ehdotukset keskittyvät nykyisen tietoturvallisuuden sääntelykehikon ongelmien korjaamiseen ja olemassa olevien säännösten tulkinnan laventamiseen.[33]

Norjan vuonna 2003 laadittu ja elinkaarensa loppuvaiheissa oleva lähinnä julkiseen sektoriin kohdistuva kansallinen tietoturvallisuusstrategia huomioi myös sääntelyn kehittämisen tarpeen. Strategia korostaa tietoturvallisuutta koskevan sääntelyn yhdenmukaista ylläpitoa ja kehittämistä, sen täytäntöönpanon kehittämistä sekä paremman perustan luomista sääntelyn kehittämiselle ja yksinkertaistamiselle. Strategia nostaa esille myös tarpeen tehdä tietoturvallisuussääntelyn kartoitus.[34] Norjan hallituksen asettaman komitea jatkaa vuonna 2006 oikeusministeriölle jättämässä mietinnössä tätä työtä ja ehdottaa sektorikohtaisia säädösmuutoksia kriittistä infrastruktuuria koskeviin säännöksiin. Samalla se myös nostaa esille tarpeen tarkemmin arvioida lainsäädäntö muutosten tarvetta.[35]

Suomessa on Ahti Saarenpään johdolla pidetty yleislain tarvetta oikeusinformatiikan tutkimuksessa toistuvasti esillä vuoden 1997 selvityksen jälkeen. Politiikan tasolla tietoturvallisuuteen liittyvän sääntelyn yleinen kehittämisen tarve on nostettu valtioneuvoston toimesta esille liikenne- ja viestintäministeriön asettaman tietoturvallisuusasioiden neuvottelukunnan työn pohjalta tehdyssä periaatepäätöksessä kansallisesta tietoturvallisuusstrategiasta. Perusoikeuksien huomioon ottaminen ja lainsäädännön vaikutusarvioinnit

---

[32] Säker information. Förslag till informationssäkerhetpolitik, Delbetänkande av InfoSäkutredningen, Stockholm 2005, SOU 2005:42, s. 22. Ehdotuksessa korostetaan myös, että valtio ei ole riittävässä määrin kehittänyt käytettävissä olevia varsin monipuolisia tietoturvallisuuden sääntelykeinoja. Vuonna 2002 asetetun selvitysmiehen toimeksiantoon, joka sai nimekseen InfoSäkutredningen, kuuluu mm. tehdä ehdotus kansallisen tietoturvallisuusstrategian luomisesta, hahmottaa Ruotsin osallistumista kansainväliseen tietoturvatyöhön sekä hahmottaa OECD:n suositusten toteuttamista kansallisesti.

[33] Selvityksessä korostetaan että yhdenmukaisen ja kattavan lainsäädäntökehikon tarve täytyy analysoida erikseen. Selvitysmiehellä ei mahdollisuutta tarvittavan kattavaan ja syväluotaavaan analyysiin. SOU 2005:42, s. 22–23.

[34] e-norge: Nasjonal strategi for informasjonssikkerhet. Utfordringer, prioriteringer og tiltak, Forsvarsdepartement, Nærings- og handelsdepartementet, Justis- og politidepartementet, juni 2003, s. 20. Vaikka sääntelyn yhdenmukaistamisen tarve on nostettu erityisen huomion kohteeksi, strategiassa sääntelyä lähdetään kehittämään kuitenkin edelleen alakohtaisesti.

[35] Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner, Norges offentlige utredninger NOU 2006:6, Oslo 2006, s. 63–68 ja 252.

olivat strategian keskeisiä kohtia.[36] Valitettavasti varsinaiset toimenpiteet ovat jääneet vähemmälle ja sulautuneet osaksi muita strategian toteuttamiseen pyrkiviä hankkeita tavalla, joka ei ole omiaan edistämään sääntelyn yleistä kehitystä[37]. Tulokset uhkaavat jäädä selvitysten tasolle.

Myös valtionhallinnon tietoturvallisuuden kehitysohjelman yhteydessä on tuotu esiin pyrkimys selvittää tarpeet ja keinot valtionhallintoa koskevan sitovan tietoturvaohjauksen tiivistämiseen. Osana selvitystä oli tarkoitus käsitellä valtionhallinnon yleisen tietoturvalain säätämisen tarve.[38] Tuore hallituksen tietoyhteiskuntastrategia vuosille 2007–2015 korostaa myös tietoturvaan liittyvän lainsäädännön ja vastuusuhteiden selkeyttä osana pyrkimystä kasvattaa luottamusta henkilötietojen suojassa pysymiseen.[39]

---

[36] Yhtenä tavoitteena valtioneuvoston periaatepäätöksessä kansallisesta tietoturvallisuusstrategiasta 4.9.2003 oli edistää kansallista kilpailukykyä ja suomalaisten tieto- ja viestintäalan yritysten toimintamahdollisuuksia. Tähän pyrittiin mm. sillä, että eri ministeriöt arvioisivat säännöllisesti tietoturvallisuuteen ja tietoyhteiskuntaan liittyvän lainsäädännön ja kansainvälisten sopimusten vaikutuksia viestintäpalvelujen, verkkopankkipalvelujen, sähköisten tunnistamispalvelujen, sähköisen kaupankäynnin ja hallinnon sähköisten asiointipalveluiden kehittämisen ja käytön kannalta sekä tekisivät tarpeen mukaan toimenpide-ehdotuksia. Myös tavoite perusoikeuksien toteutumisen turvaamisesta liittyi oleellisesti lainsäädännön kehittämisen. Periaatepäätöksen mukaan kaikkien viranomaisten tulisi huolehtia siitä, että sananvapaus, viestinnän luottamuksellisuus, yksityisyyden suoja ja muut perusoikeudet huomioidaan tietoyhteiskunnan palveluita, sähköistä viestintää ja tietoturvallisuutta käsittelevissä säännöksissä, viranomaisohjeissa ja standardeissa sekä viranomaisten sähköisissä asiointipalveluissa.

[37] Ks. tietoturvallisuusstrategian 14.12.2004 ja 13.12.2005 päivätyt seurantaraportit. Kansallisen tietoturvallisuusasioiden neuvottelukunnan sihteeristö: Tietoturvalliseen tietoyhteiskuntaan: Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 14.12.2004, Liikenne- ja viestintäministeriö, Ohjelmia ja strategioita 1/2004, s. 9, saatavilla osoitteessa http://www.mintc.fi/ [27.9.2006] sekä Kansallisen tietoturvallisuusasioiden neuvottelukunnan sihteeristö: Tietoturvalliseen tietoyhteiskuntaan: Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 13.12.2005, Liikenne- ja viestintäministeriön julkaisuja 93/2005, s. 8 ja 39–41, saatavilla osoitteessa http://www.mintc.fi/ [27.9.2006].

[38] Valtiovarainministeriön alaisen Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) vastuulla oleva valtionhallinnon tietoturvallisuuden kehitysohjelma pyrkii osaltaan konkretisoimaan kansallista tietoturvastrategiaa sekä edistämään sen toteutumista erityisesti julkishallinnossa. Yksi kehitysohjelman keskeisistä hankkeista on valtionhallinnon tietoturvatyön yleinen tukeminen, johon myös sääntelyn kehittäminen liittyy. Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006, Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI 1/2004, Valtiovarainministeriö, hallinnon kehittämisosasto, Helsinki 2004, s. 46.

[39] Hallituksen tietoyhteiskuntaohjelma, Uudistava, ihmisläheinen ja kilpailukykyinen Suomi: Kansallinen tietoyhteiskuntastrategia 2007–2015, syyskuu 2006, Tietoyhteiskuntaohjelmat, valtioneuvoston kanslia, s. 12, saatavilla osoitteesta http://www.tietoyhteiskuntaohjelma.fi/ [27.9.2006].

Varsinaiset toimenpiteet jäävät kuitenkin nähtäväksi. En pidä yleislain säätämistä mitenkään todennäköisenä. Perusteet ovat samat kuin sääntelyn määrän vähentämistä koskevien hankkeiden yhteydessä.[40] Yhtenäistettävien säännösten määrä on niin suuri ja monikerroksinen, että jo pelkkä kaiken tietoturvallisuuteen liittyvän lainsäädännön hahmottaminen kansallisesti on vaikeaa. Lainvalmistelussa vaadittava työmäärä on huomattava. Samalla lainvalmistelijat ovat sidottuja lyhyen ajan suppeisiin säädösmuutoksiin ja erityisesti jo voimassa olevien lakien muutoksiin toimintaympäristön muuttuessa. Niukkoja resursseja ei kovin helposti kohdisteta pitkän linjan hankkeisiin, joissa yhtenäistettävien intressien määrä on suuri ja onnistuminen epävarmaa.[41]

Yhden niin julkiseen kuin yksityiseenkin sektoriin kohdistuvan yleislain säätäminen ei kuitenkaan ole ainoa keino selkeyttää sääntelyä ja saavuttaa yhtenäisyyttä. Tuloksia on jo saavutettu kokoamalla yhteen tietoturvallisuuden sääntelyä henkilötietoja käsiteltäessä, sähköisen viestinnän yksityisyyden suojan osalta, sekä viranomaistoiminnan julkisuuden ja sähköisen asioinnin järjestämisessä.[42]

Kansainvälisestikin on nähtävissä, että sähköistä hallintoa ja hallinnon julkisuutta sekä henkilötietoja koskevat säännökset ovat kehittymässä suuntaan, jossa ne osoittavat tietoturvallisuuden peruslähtökohdat ja toimivat näin osaltaan tietoturvallisuuden yleislakeina.[43] Euroopan ulkopuolella tätä kehityslinjaa edustavat muun muassa Yhdysvaltain tietoturvallisuuden hallintaa liittovaltiotasolla koskeva laki vuodelta 2002 (Federal Information Security Management Act of 2002, ”FISMA”).[44]

Sektorikohtaiset yleislait eivät kuitenkaan, kuten ei edes yhden niin julkiseen kuin yksityiseenkin sektoriin kohdistuvan yleislain säätäminenkään,

---

[40] Ks. *Tala*: Oikeussääntelyn määrä ja vaihtoehdot, s. 60.

[41] Selitys liittyy *Tuomas Pöystin* kehittämään realistiseen teoriaan oikeuden niukkuudesta johon ajatus lainsäädäntövallan rajallisuudesta kytkeytyy. Katso esim. *Pöysti*: Communicational Quality of Law – a Legal Informatics Perspective, s. 471–479, i Cecilia Magnusson Sjöberg och Peter Wahlgren (red.): Festskrift till Peter Seipel, Stockholm 2006, s. 463–495.

[42] Kehitys on linjassa lainsäädäntötutkimuksessa laajemminkin tehdyn huomion kanssa siitä, että eniten tuloksia sääntelyn eriytymisen ja sirpaloitumisesta johtuvien haittojen vähentämisessä on saavutettu kokoamalla yhteen samaa asiaa tai aihetta koskevaa sääntelyä lakiuudistuksen yhteydessä. Huomion tekee muun muassa *Tala*: Oikeussääntelyn määrä ja vaihtoehdot, s. 59.

[43] Tämän kehityslinjan on tuonut esiin myös *Tuomas Pöysti* systematisoidessaan keskeisiä eurooppalaisia tietoturvallisuussäännöksiä artikkelissaan ICT and Legal Principles, s. 598.

[44] FISMA on osa yleistä sähköisen hallinnon lakia (E-Government Act of 2002, Public Law No. 107-347).

sinällään ole tae yhtenäisyyden saavuttamiselle ja säilymiselle. Erityislakien säätäminen tiettyjen alojen intressejä varten voi eriyttää sääntelyä ja hajaannuttaa tulkintoja yleislaista huolimatta. Henkilötietojen kasvava sääntely henkilötietolain tosiasiallista merkitystä henkilötietojen käsittelyn yleislakina hämärtävien erityislakien kautta on tästä selkeä osoitus.[45]

LAINSÄÄDÄNNÖN LAADUN KEHITTÄMINEN

Tiukan lakisääteisyyden aiheuttamien ongelmien pienentäminen yleislain säätämisen ja oikeustieteen kehittymisen kautta tulee olemaan pitkällinen prosessi. Mikäli tietoturvallisuuden politiikkalinjauksissa esitetty sääntelyn kehittäminen ja yhdenmukaistaminen aiotaan saavuttaa lyhyemmällä tähtäimellä, on julkisen vallan syytä lähteä kehittämään ratkaisukeinoja hieman vaatimattomammasta lähtökohdasta.

Yleislain säätäminen ei ole lainsäätäjän ainoa, eikä edes ensisijainen keino koherenssin aikaansaamiseksi. Kuten yllä on jo huomautettukin, lainsäätämismenettelyyn kuuluu käytäntöjä, jotka pyrkivät varmistamaan uuden lainsäädännön sisäisen rationaalisuuden. Tietoturvallisuuden sääntelyssäkin näiden rooli on ollut merkittävä. Sähköisen viestinnän tietosuojalain valmistelun yhteydessä tehdyt laajat perusoikeusanalyysit ovat tästä selkeä esimerkki.

Näiden oikeudellisten käytäntöjen merkitys sääntelyn laadun parantamisessa on sinällään varsin vakiintunut. Keskeisiä tietoturvallisuuteen liittyviä kehitystarpeita ei ole nähtävissä. En mene näiden oikeudellisten käytäntöjen käsittelyssä tämän pidemmälle. Lainsäädännön laadun parantamisessa pyrkimyksenä onkin yleensä ollut kehittää käytäntöjä näiden toimijoiden työn tueksi.

OECD pitää jäsenmailtaan kokoamiensa lainsäädännön laadun parantamiseen pyrkivien hankkeiden kokemusten kautta välttämättöminä toimenpiteinä ainakin sääntelyn vaikutusten arvioinnin kehittämistä, julkisen konsultaation edistämistä ja lainsäädäntömenettelyn julkisuutta, sekä sääntelyn

[45] Siinä missä tietoturvallisuudessa lainsäädännön sirpaloituminen on tapahtunut yleislain puuttuessa, on henkilötietojen suojan osalta kehitys kulkenut henkilötietolain tosiasiallista merkitystä henkilötietojen käsittelyn yleislakina hämärtävien erityislakien kautta. Tätä henkilötietojen sääntelyn kehitystä on *Ahti Saarenpää* kuvannut useaan otteeseen (esim. Verkkoyhteiskunnan oikeutta – johdatusta aiheeseen, s. 9; E-government and Good Government, s. 249).

vaihtoehtojen harkintaa.[46] Monia ratkaisuehdotuksia on tehty myös pohjoismaisessa oikeusinformatiikan tutkimuksessa. Erityisesti on keskitytty lainsäädännön kommunikatiivisen puolen kehittämiseen ja uusien lähestymistapojen löytämiseen.[47] Näiden käyttöönotto ja kehittäminen jatkuu.

Tässä yhteydessä on syytä nostaa esille yksi keskeinen suomalaisissa lainvalmistelun laadun parantamiseen pyrkivissä hankkeissa esiin noussut ajatus, jolla tietoturvallisuuden sääntelyn laatua voitaisiin kattavasti parantaa ja yhdenmukaistaa. Kyse on *vaikutusten arvioinnin* kehittämisestä.

Vuonna 2004 uusittuihin hallituksen esitysten laatimisohjeisiin (HELO) kirjattiin edellytys siitä, että esityksen vaikutukset tietoyhteiskuntaan, sen kehittymiseen sekä *tietoturvaan* on selostettava osana vaikutusten arviointia.[48] Ajatus on hieno. Tietoturvallisuus ei ole vain muutaman oikeudenalan kysymys. Tietoturvallisuuden näkökulma läpäisee koko oikeusjärjestyksen ja sisältää lisäksi kirjavan joukon erilaisia lähtökohtia. Tietoturvallisuutta koko yhteiskunnan kattavana politiikkana ei voida kehittää, jos jollakin sääntelyn alalla luodaan negatiivisia kannustimia.

Tietoturvallisuus on, kuten strategioiden ja periaatepäätösten lukuisuus sinällään osoittavat, merkittävä verkkoyhteiskunnan tavoitetila – julkinen hyvä, jota ilman perusrakenteet sortuvat. Ajatus siitä, että lainsäädännön ja sääntelyn yleensä tulisi edistää tietoturvallisuutta sekä kannustaa sen kehittämiseen tai vähintäänkin pidättäytyä haittaamasta sen kehitystä, on selkeä. Vaikutukset tietoturvallisuuteen tulisikin ottaa huomioon luotaessa uutta sääntelyä kaikilla oikeuden alueilla, eikä vain valmisteltaessa nimenomaan tietoturvallisuuteen liittyvää lainsäädäntöä riippumatta siitä, ovatko mahdolliset vaikutukset sitten välillisiä vai välittömiä.

---

[46] OECD on koonnut yhteen ja analysoinut eri maiden kokemuksia näiden menetelmien käytöstä muun muassa julkaisussaan Regulatory Policies in OECD Countries: From Interventionism to Regulatory Governance, OECD Reviews of Regulatory Reform, OECD, Paris 2002, s. 43–73.

[47] *Peter Wahlgren*: IT and Legislative Development, in Peter Wahlgren (ed.): IT Law, Scandinavian studies in law 47, Stockholm Institute for Scandinavian Law, Stockholm 2004, s. 601–619) kokoaa lyhyesti yhteen jo käytettyjä menetelmiä ja alustavasti kartoittaa mahdollisia uusia keinoja, joilla lainsäädäntömenettelyä voitaisiin tukea nopean muutoksen leimaamassa monimutkaisessa teknisessä toimintaympäristössä. *Tuomas Pöysti* kehittää oikeuden viestinnällisen laadun yleisiä edellytyksiä artikkelissaan Communicational Quality of Law, s. 463–495.

[48] Valtioneuvosto, Hallituksen esityksen laatimisohjeet, Oikeusministeriön julkaisuja 2004:4, Helsinki, s. 17, saatavilla osoitteesta http://www.om.fi/Etusivu/Julkaisut/Julkaisusarjat/Oikeusministerionjulkaisuja/Julkaisujenarkisto/ [11.10.2006].

Tekijänoikeuslainsäädäntö on varoittava esimerkki. Tekijänoikeuden teknisten suojamenetelmien kiertämisen kiellon, erityisesti niiden valmistamisen ja levittämisen kiellon vaikutukset tietoturvallisuuden tutkimukseen yleisesti ja haavoittuvuusanalyysiin erityisesti jäivät laajalti näkemättä säädösten valmistelu vaiheessa. Kokemukset Yhdysvaltojen vastaavista säädöksistä (Digital Millennium Copyright Act, DMCA)[49] kuitenkin osoittavat, että säännöksiä on käytetty nimenomaan tietoturvallisuustutkijoiden tutkimustulosten julkaisun estämiseen.[50] Myös teknisten suojamenetelmien käytön vaikutukset informaatiohyödykkeiden, kuten ohjelmistojen, laatuun ja käytettävyyteen jäi pitkälti näkemättä.[51] Näin vaikka kyse on keskeisestä kuluttajansuojan kysymyksestä. Vaikutukset tietoturvallisuuteen olisi ollut syytä ottaa vakavammin huomioon jo lainsäädäntöä valmisteltaessa.

Valitettavasti HELO-ohjeisiin kirjattu lausuma tietoturvavaikutusten selostamisesta on jäänyt pitkälti pelkäksi periaatteelliseksi osoitukseksi tietoturvallisuuden tärkeydestä. Koko ohjeiden käyttö on jäänyt lainvalmistelussa vähäiseksi, kuten Valtioneuvoston lainvalmistelun suunnittelun ja johtamisen kehittämistyöryhmä (lainvalmistelun kansliapäällikköryhmä) on mietinnössään huomauttanut.[52] Uuteen kansalliseen tietoyhteiskuntastrategiaan on myös yhdeksi toimenpiteeksi yhteentoimivaa ja esteetöntä tietoyhteiskuntainfrastruktuuria koskevassa painopistealueessa kirjattu tietoyhteiskuntavaikutusten arvioinnin liittäminen vakiintuneeksi osaksi säädösvalmisteluprosessia.[53]

---

[49] Digital Millennium Copyright Act of 1998, Public Law No. 105-304, 17 U.S.C, Sec.1201.

[50] Vaikutuksia on kuvannut erityisesti Yhdysvaltalainen voittoa tavoittelematon kansalaisoikeusjärjestö Electronic Frontier Foundation (EFF) julkaisussaan Unintended Consequences: Five Years under the DMCA, v. 4, huhtikuu 2006, otsikko ”Chilling Free Expression and Scientific Research”, osoitteessa http://www.eff.org/IP/DMCA/[11.10.2006].

[51] Sony-BMG:n käyttämän CD:n kopionesto-ohjelmien ”rootkit”-haavoittuvuus on näistä vaikutuksista kenties paljastavin esimerkki. Ohjelmat muun muassa lähettävät tietoja CD:n kuuntelusta eteenpäin sekä asentavat ilmoittamattomia ja joissakin tapauksissa piilotettuja tiedostoja käyttäjänsä koneelle avaten mahdollisuuksia tietomurroille. Tapausta on kuvannut muun muassa EFF verkkosivuillaan osoitteessa http://www.eff.org/IP/DRM/Sony-BMG/ [11.10.2006].

[52] Valtioneuvoston lainvalmistelun suunnittelun ja johtamisen kehittämisryhmän mietintö (Lainvalmistelun kansliapäällikköryhmä), *Tehokkaampaa, suunnitelmallisempaa ja hallitumpaa lainvalmistelua*, Valtioneuvoston kanslian julkaisusarja 13/2005, s. 211–212, saatavilla osoitteessa http://www.vnk.fi/julkaisut/ [11.10.2006]. Vaikutusten arvioinnin pieni rooli lainsäädännön laadun parantamisessa Suomessa on saanut osakseen kritiikkiä ja kehitysehdotuksia myös OECD maakohtaisissa sääntelyn uudistusta koskevissa raporteissa. OECD: Government Capacity to Assure High Quality Regulation in Finland, s. 33–37.

[53] Hallituksen tietoyhteiskuntaohjelma: Uudistuva, ihmisläheinen ja kilpailukykyinen Suomi, s. 26.

Jo sinällään tämä kertoo jotain HELO-ohjeisiin kirjatun lausuman vähäisestä käytännön merkityksestä. Huolestuttavampaa on se, että vaikutukset tietoturvaan on unohdettu kokonaan.

Hieman toisesta näkökulmasta tietoturvallisuuteen liittyvien vaikutusten arviointeja on ehdottanut valtioneuvosto periaatepäätöksessään kansallisesta tietoturvallisuusstrategiasta, kuten jo yllä on esitetty. Alkuperäisenä tavoitteena oli, että eri ministeriöt arvioisivat säännöllisesti tietoturvallisuuteen ja tietoyhteiskuntaan liittyvän lainsäädännön ja kansainvälisten sopimusten vaikutuksia sähköisten palvelujen kehittämisen ja käytön kannalta sekä tekisivät tarpeen mukaan ehdotuksia toimenpiteistä.

Vaikka lähtökohta oli käänteinen HELO-ohjeissa esitetylle vaatimukselle jokaisen hallituksen esityksen yhteydessä tehtävästä tietoturvallisuuteen kohdistuvien vaikutusten arvioinnista, eli tavoitteena oli arvioida vaikutuksia sähköisten palvelujen kehittämiseen valmisteltaessa tietoturvallisuuteen liittyvää lainsäädäntöä, oli ajatus oikean suuntainen. Valitettavasti varsinaiset toimenpiteet ovat jääneet vähemmälle ja sulautuneet osaksi muita strategian toteuttamiseen pyrkiviä hankkeita tavalla, joka ei ole omiaan edistämään sääntelyn yleistä kehitystä[54]. Tulokset uhkaavat jäädä selvitysten tasolle.

Lisäongelmia tällaiselle kattavalle tietoturvallisuusvaikutusten analyysille lainvalmistelussa muodostuu tietoturvallisuuden asiantuntemuksen saamisesta mukaan lainvalmisteluun. Lainvalmistelijoilta itseltään tällaista on kohtuutonta olettaa. Ulkopuolisten asiantuntijoiden ääni uhkaa jäädä kuulumatta samalla, kun luovutaan perinteisestä komiteakäytännöstä lainvalmistelussa. Siirryttäessä kohden eurooppalaista lobbauksen kautta vaikuttamista ei tietoturvallisuuden asiantuntijoiden ääni välttämättä pääse esiin.[55] Eritoten näin uhkaa käydä vaikutusten arviointien osalta.

---

[54] Ks. yllä viitatut tietoturvallisuusstrategian 14.12.2004 ja 13.12.2005 päivätyt seurantaraportit. Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 14.12.2004, s. 9, sekä kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 13.12.2005, s. 8 ja 39–41.

[55] Kuten *Pekka Hallberg* (The Rule of Law, Helsinki 2004, s. 286–288) tuo esiin, viitaten *Peter Bouwenin* tutkimuksiin lobbauksen teoreettisesta viitekehyksestä EU:ssa (Corporate lobbying in the European Union: the logic of access, Journal of European Public Policy, 9(3): 365–390, 2002, sekä A Comparative Study of Business Lobbying in the European Parliament, the European Commission and the Council of Ministers, Max-Planck Institut für Gesellschaftsforschung Discussion Paper 02/7, 2002), yksityisen sektorin hallussa oleva asiantuntijatieto on yksi keskeisistä korvaamattomista kauppatavaroista, joilla lobbaajat pääsevät vaikuttamaan päätöksentekoon.

Sinällään paljon käytetyt hallitusten esitysten laajat lausuntokierrokset eivät tuo asiantuntijoita mukaan vaikutusten arviointiin, sillä vaikutusten arviointeja edelleen harvoin lähetetään lausuntokierroksille.[56] Lisäksi meiltä puuttuvat edelleen aktiiviset ja tarpeeksi vaikutusvaltaiset tietoyhteiskunnan kansalais- ja asiantuntijajärjestöt, jotka kokoaisivat asiantuntijoiden näkemyksiä lainvalmistelun tarpeisiin.

Toivo tietoturvallisuuteen kohdistuvien vaikutusten arvioinnin kehittämisestä HELO-ohjeiden mukaisesti, ja erityisesti tarvittavan asiantuntijatuen järjestämisestä lähitulevaisuudessa, on olemassa. Valtiovarainministeriö ja kauppa- ja teollisuusministeriö ovat parhaillaan selvittämässä vaihtoehtoja säädösten vaikutusarvioinnin asiantuntijatuen järjestämisestä.[57] Toivottavasti myös tietoturvallisuuden asiantuntemus tulee olemaan mukana valittavassa toimintamallissa. Tilaisuus on liian herkullinen jätettäväksi käyttämättä. Huomioiden erityisesti, että pyrkimyksenä ei ole kehittää pelkästään lainsäädännön vaikutusten analysointia, vaan myös säädöksille vaihtoehtoisten ohjauskeinojen vaikutusten arviointia.

VIELÄ OIKEUSTIETEEN ROOLISTA

Monista lainsäätäjän käytettävissä olevista sääntelyn laadun parantamiseen tähtäävistä käytännöistä huolimatta lainsäädäntömenettelyssä oikeuden sisäinen rationaalisuus on alistettu kohderationaalisuudelle, lainsäädännölle asetettujen tavoitteiden toteutumiselle, jota poliittisen lainsäätäjän tavoiterationaalinen näkökulma korostaa.[58] Näin erityisesti tietoturvallisuudesta säädettäessä, sillä oikeudenalan kehitys on ollut pitkälti lyhyen aikavälin poliittisten tavoitteiden ajamaa. Tästä syystä muiden oikeuden sisäistä rationaalisuutta ylläpitävien oikeudellisten käytäntöjen, kuten lainkäytön ja oikeustieteen, rooli on korostunut.

Samasta syystä pelkkä lainsäädännön laadun korostaminen ja lainsäätämiskäytäntöjen kehittäminen paremmin oikeuden sisäistä rationaalisuutta huomioon ottavaksi ei ole riittävää. Niin merkittävää kuin lainsäädännön laadun parantaminen ja lainvalmistelun edellytysten kehittäminen onkin,

---

[56] OECD nostaa epäkohdan esiin maakohtaisessa sääntelyn uudistusta koskevassa raportissaan. OECD: Government Capacity to Assure High Quality Regulation in Finland, s. 36.

[57] Valtiovarainministeriön tiedote 94/2006, 15.9.2006, osoitteessa http://www.vm.fi/vm/fi/03_tiedotteet_ja_puheet/ [11.10.2006].

[58] *Tuori*: Kriittinen oikeuspositivismi, s. 154.

emme voi tyytyä tietoturvallisuudessa vain niihin. Yleislain vaihtoehto on edelleen syytä pitää esillä ja oikeustieteen on jatkettava tietoturvallisuuden yleisten oppien kehittelyä. Ilman yleisten oppien selkeää muotoilua ei sääntelyn tietoturvallisuuteen kohdistuvien vaikutusten arviointiakaan ole mahdollista suorittaa asianmukaisesti. Mitäpä muuta oikeustieteilijä voi korostaa kuin oikeustieteen merkitystä?

EPILOGI

Tietoturvallisuuden sääntelyn analyysissä ei kuitenkaan ole mahdollista pitäytyä vain kansallisen lainsäädännön tai sitä alemmanasteisen sääntelyn tarkastelussa. Sääntely on välttämättä kansainvälistä ja näkökulmaa on laajennettava perinteisestä valtiokeskeisestä lähtökohdasta. Tällöin esiin nousee monia vaihtoehtoisia sääntelykeinoja, joiden käyttöönottoa kirjoitetun lain asemaa korostava lakipositivistinen perusasenne rajoittaa.

Vahvan legalistinen sääntelykulttuurimme yhdistettynä oikeudellisen koulutuksen saaneiden vahvaan asemaan lainvalmistelussa, vuoden 2000 perustuslain tiukkaan lakisääteisyyden vaatimukseen perusoikeuksista säädettäessä sekä perusoikeuksien horisontaalivaikutusten laajenemiseen, on saanut aikaan selkeiden, yksityiskohtaisten ja täsmällisten eduskuntalakien käytön merkittävän aseman sääntelykulttuurissamme. Tämä on osittain ollut haitaksi vaihtoehtoisten sääntelykeinojen käyttöönotolle ratkaisuna sääntelyn määrän kasvun aiheuttamiin ongelmiin.[59] Tyydyn tässä vain nostamaan asian esiin. Siihen on syytä palata myöhemmin.

---

[59] Oikeudellisen sääntelyn vaihtoehdoilla tarkoitan perinteisestä komenna ja valvo (command and control) -tyyppisestä sääntelystä, jossa eri toimijoita koskevat verraten yksityiskohtaiset, monesti pakottavat säännökset, joihin kohdistuu viranomaisvalvontaa ja joiden noudattamista tehostetaan yleensä negatiivisilla sanktioilla, poikkeavia sääntelymalleja. Eri sääntelymallien jaotteluista lyhyesti, ks. *Jari Råman*: Regulating Secure Software Development, Rovaniemi 2006, s. 167–174. Vaihtoehtoisten sääntelykeinojen kehittämisen kannalta kritiikkiä legalistinen sääntelykulttuurimme ja uuden perustuslain mukanaan tuoma laajentunut lakisääteisyyden vaatimus ovat saaneet osakseen erityisesti OECD:n Suomea koskeneessa raportissa Government Capacity to Assure High Quality Regulation in Finland, s. 30–32. Kritiikkiä oikeussääntelyn vaihtoehtojen riittämätön käyttö on saanut osakseen myös niin lainsäädäntö tutkimuksessa (*Tala*: Oikeussääntelyn määrä ja vaihtoehdot, s. 103; sekä *sama*: Lainsäädännön vaihtoehdot – tarve ja tehtävät, teoksessa Heidi Lindfors (ed.) Lainsäädäntöä vai muuta oikeudellista ohjailua, Oikeuspoliittisen tutkimuslaitoksen tutkimustiedonantoja 67, Helsinki 2005) kuin politiikankin tutkimuksessa (*Hallberg*: The Rule of Law, s. 279). Muita keskeisiä syitä oikeussääntelyn vaihtoehtojen käytön vähäisyydelle ovat muun muassa puutteet ohjeissa, koulutuksessa ja organisatorisessa tuessa.