Lasse Tyry

Tietoturvallisuudesta osana hyvän sähköisen hallinnon säännöstöä

Johtamisen akateeminen yksikkö
Julkisoikeuden pro gradu -tutkielma
Hallintotieteiden maisteri

Vaasa 2024

VAASAN YLIOPISTO
Johtamisen akateeminen yksikkö
Tekijä: Lasse Tyry
Tutkielman nimi: Tietoturvallisuudesta osana hyvän sähköisen hallinnon säännöstöä
Tutkinto: Hallintotieteiden maisteri
Oppiaine: Julkisoikeus
Työn ohjaaja: Kristian Siikavuori
Valmistumisvuosi: 2024 **Sivumäärä:** 80

TIIVISTELMÄ:
Digitalisaation vaikutuksesta tiedon muuttuessa sähköiseen muotoon ovat sähköiset järjestelmät ja tietovarannot nousseet elintärkeään rooliin verkkoyhteiskunnan viranomaistoiminnassa. Sähköistyminen ja globaalit verkot ovat tuoneet uusia turvallisuusuhkia, jonka seurauksena on myös viranomaisen tietoturvallisuuden roolista alettu keskustella. Tietoturvallisuuteen liittyvässä keskustelussa osana sähköistä hallintoa on hahmotettu etenkin hyvän hallinnon säännöstön kautta. Digitalisaation tuoman sähköistymisen hyödyntäminen on mahdollistanut hallintoon merkittäviä mahdollisuuksia etenkin tehokkuuden kannalta, mutta miten julkinen hallinto ja lainsäädäntö pystyvät vastaamaan tietoturvallisuuden nopeatempoiseen ympäristöön?

Tässä tutkielmassa tarkastellaan tietoturvallisuuden sääntelyä viranomaistoiminnassa sekä tietoturvallisuuden suhdetta hyvän hallinnon osatekijöihin. Tutkielma keskittyy tarkastelemaan tietoturvallisuuden viranomaissääntelyä erityisesti uuden tiedonhallintalain säännöstön kautta sivuten myös muita tietoturvallisuudesta säädettyjä säädöksiä. Tutkielmassa käsitellään tietoturvallisuuden suhdetta hyvän hallinnon osatekijöihin perustuslaissa ja hallintolaissa ilmenevien tekijöiden kautta. Tutkielmassa haetaan vastausta kahteen tutkimuskysymykseen. Ensimmäisenä tutkimuskysymyksenä on, miten kansallinen lainsäädäntö velvoittaa viranomaista huolehtimaan tietoturvallisuudesta sekä mistä tietoturvallisuus oikeudellisena käsitteenä koostuu? Toisena tutkimuskysymyksenä on, millaisen käsitesisällön sekä roolin tietoturvallisuus saa osana hyvän hallinnon tunnusmerkistöä sekä laajemmin mahdollisena perusoikeutena?

Tutkielman tutkimusmetodina on lainoppi, jonka avulla tulkitaan ja systematisoidaan voimassa olevaa oikeutta. Tutkielma sijoittuu oikeusinformatiikan, tarkemmin informaatio-oikeuden tutkimukseen pitäen sisällään kuitenkin vaikutteita hallinto-oikeudellisesta tutkimuksesta viranomaisen tietoturvallisuussääntelyn osalta.

Tutkielmassa hahmotetaan tietoturvallisuutta oikeudellisena käsitteenä ja sen sisältöä. Oikeudellisena käsitteenä tietoturvallisuus ilmenee etenkin tiedon laadullisten ominaisuuksien eli saatavuuden, eheyden ja luottamuksellisuuden kautta. Tutkielmassa osoitetaan, että tietoturvallisuuden asianmukaisella toteuttamisella on huomattava yhteys hyvän hallinnon eri osatekijöiden toteutumiselle. Tutkielmassa tietoturvallisuuden suhdetta tarkastellaan etenkin hyvän hallinnon julkisuuden, palveluperiaatteen, viranomaisten yhteistyön ja neuvonnan kautta. Hyvän hallinnon turvaamiseksi etenkin digitaalisessa toimintaympäristössä tietoturvallisuuden kokonaisvaltainen turvaaminen saatavuuden, eheyden ja luottamuksellisuuden osalta nousee keskeiseen asemaan. Lisäksi tutkielmassa käsitellään laajemmin tietoturvallisuuden yhteyksiä perus- ja ihmisoikeuksien toteutumiseen ja niiden turvaajana.

AVAINSANAT: Tietoturvallisuus, hyvä hallinto, verkkoyhteiskunta, digitaaliset palvelut, digitalisaatio

Sisällys

Lyhenteet

DpL	Laki digitaalisten palvelujen tarjoamisesta (306/2019)
HaL	Hallintolaki (434/2003)
Julkisuuslaki	Laki viranomaisten toiminnan julkisuudesta (621/1999)
Mom.	Momentti
PeL	Suomen perustuslaki (731/1999)
SVPL	Laki sähköisen viestinnän palveluista (917/2014)
TiHL	Laki julkisen hallinnon tiedonhallinnasta (906/2019)

1 Johdanto

1.1 Tietoturvan ja hyvän hallinnon muuttuva ympäristö

Digitalisaation aikaansaama perustavalaatuinen yhteiskunnallinen ja tekninen muutos on vaikuttanut kauttaaltaan elämämme jokaisella alueella. [1] Tietokoneiden laskentatehon lähes eksponentiaalinen kehitys 1960-luvusta lähtien on mahdollistanut valtavien tietomäärien nopean käsittelyn sekä arkistoinnin muutamassa vuosikymmenessä [2] . Myös julkishallinto on tullut erinäisistä tietojärjestelmistä ja tietokoneista sekä niiden virheettömästä toiminnasta riippuvaiseksi järjestäessään julkisia palveluita sekä omaa sisäistä toimintaansa[3]. Nykyistä digitaalisen muutoksen vaikutusta yhteiskuntaan voidaan kuvata tarkemmin verkkoyhteiskunnan käsitteellä[4]. Verkkoyhteiskunnalla kuvataan tietoteknisesti ja viestinnällisesti erinäisiin tietojärjestelmiin ja tietoverkkoihin sitoutunutta ja niiden varassa toimivaa yhteiskuntaa[5].

Digitalisaatio ja teknologinen murros nostavat esiin uudenlaisia oikeudellisia kysymyksiä, jotka eivät ainoastaan tuota uudenlaisia sääntelyn kohteita, vaan myös muuttavat oikeudellisen ratkaisutoiminnan käytänteitä[6]. 2000-luvulla on säädetty useita kokonaan uusia säädöskokonaisuuksia jäsentämään digitalisaation vaikutuksia sekä uudistettu jo vanhoja säädöksiä digitaalista todellisuutta palveleviksi. Näistä uusista sääntelykokonaisuuksista yhtenä merkittävimpänä oikeudellisena kysymyksenä ovat eittämättä tietoturvallisuuteen liittyvät asiat.

---

[1] Parviainen & al. 2017. S. 19 Digitalisaatio käsitetään toimintatapojen muutoksena, jossa digitaalisia ratkaisuja hyödynnetään laajamittaisesti yksilön, organisaation ja yhteiskunnan toiminnassa.
[2] Ks. Gordon Mooren mukaan nimetty ”Mooren laki”.
[3] Valtioneuvoston periaatepäätöksessä LVM/2021/44, s. 3 kuvataan tietojärjestelmien toimivuuden ja tietoturvallisuuden roolia seuraavasti: ”Yhteiskunnan eri sektorit ovat yhä riippuvaisempia digitaalisten palveluiden käytöstä niin Suomessa kuin maailmanlaajuisesti. Yhteiskunnan keskeiset palvelut, kuten sähkön ja juomaveden jakelu sekä terveydenhuollon palvelut, tarvitsevat luotettavia yhteyksiä ja tietojärjestelmiä toimiakseen… käytössä olevien yhteyksien, palveluiden ja laitteiden tietoturvallisuuden taso vaikuttaa suoraan kansalaisten digitaalisia palveluita ja tuotteita kohtaan kokemaan luottamukseen.”
[4] Saarenpää, 2000, s. 3-5
[5] Saarenpää & Riekkinen, 2023, s. 41
[6] Nuotio, 2020, s. 509

Tätä digitalisaation ja oikeuden välistä suhdetta Saarenpää (2023) kuvaa oikeudellisena digitaalisena verkkoyhteiskuntana, jonka keskeisiä tunnusmerkkejä ovat muun muassa perusoikeuksien siirtyminen verkkovaikutteisiksi ja verkoissa hyödynnettäviksi, informaation ja sen käsittelyn oikeudellisesti muuttunut asema yhteiskunnassa, sähköiset palvelut ja sähköinen asiointi sekä tietoturvallisuuden entistä tärkeämpi rooli oikeuksiemme toteutumisessa ja yleisimmin yhteiskunnan rakennetekijänä[7].

Tietoturvallisuuden hallinta julkishallinnossa vaikuttaa julkisten tehtävien tehokkuuteen, luotettavuuteen ja laatuun. Tietoturvallisuuden tehokas hallinta ja turvaaminen vaatii kuitenkin varsin kompleksista lähestymistä, jonka keskiössä ovat etenkin oikeudelliset laintasoiset säännökset, menettelylliset ja organisatoriset määräykset vastuunjaosta, fyysiset ja tekniset suojatoimenpiteet, henkilöstön osaaminen sekä muut organisaation resurssit jotka vaikuttavat tietoturvallisuuden hallintajärjestelmän tehokkuuteen.[8] Erityisesti sähköisen hallinnon ja sen perustana olevien tietoverkkojen tietoturva- ja yksityisyyskysymykset ovat nousseet hallitusten ja julkishallinnon suurimmiksi huolenaiheiksi[9]. Julkishallinnon huolenaiheet tietoturvallisuudesta ovat aiheelliset, sillä julkinen sektori on yksi suurimmista sektoreista joihin kohdistuu vakavia kyberhyökkäyksiä[10]. Etenkin sähköisen hallinnon suurin operatiivinen haaste onkin epäilemättä kyberturvallisuus, mukaan lukien yksityisyyteen ja tietojärjestelmiin kohdistuvat uhat[11]. Julkisen sektorin tietoturvallisuusuhkiin on lähiaikoina herätty laajasti myös Suomessa ja siihen liittyvät teemat ovat olleetkin keskeisesti esillä niin Juha Sipilän, Sanna Marinin ja Petteri Orpon hallitusten työskentelyssä[12].

[7] Saarenpää & Riekkinen, 2023, s. 49
[8] Szczepaniuk ja muut, 2020, s. 1, 7
[9] Dawes, 2008, S. 92
[10] ITU, 2015, s. 72
[11] Andreasson, 2012, s. 5
[12] VM/2500/00.01.00.01/2017, s.1: Sipilän hallituksen Digitalisoidaan julkiset palvelut kärkihankkeen päätoimenpiteisiin kuului uuden tiedonhallintalain valmistelu. VN 2019:31: Marinin hallituksen hallitusohjelmassa kyberturvallisuus esiintyy keskiössä sekä Marinin hallitus toteutti kyberturvallisuuden kehittämisohjelman (LVM 2021:7). Orpon hallitusohjelmassa VN 2023:58 kyberturvallisuus esiintyy keskeisenä kehityskohteena, sekä hallituksen on määrä uudistaa kansallista kyberturvallisuusstrategiaa.

Hallinnossa tapahtunut ja edelleen jatkuva digitalisaation murros vaikuttaa myös olennaisesti hyvän hallinnon tarkasteluun. Oikeudellisessa digitaalisessa verkkoyhteiskunnassa hyvän hallinnon käsite on saanut uusia ulottuvuuksia ja muokannut jo entuudestaan tunnistettuja hyvän hallinon takeiden toteutustapoja. Näin on käynyt esimerkiksi julkisuuden toteuttamisessa, kun viranomaisen tiedottaminen on pitkälti siirtynyt painetusta lehdestä verkkoon. Viranomaisten toiminnan tukeutuessa pitkälti tietojärjestelmien ja tietokoneiden varaan, herääkin kysymys tietoturvallisuuden roolista laajemmin osana perusoikeuksien toteutumisesta sekä osana hyvää hallintoa.

1.2 Tutkimuskysymykset, rajaus ja metodit

Tutkimukseni käsittelee sitä, miten kansallinen lainsäädäntö säätelee viranomaisen tietoturvallisuusvaatimuksia ja miten tietoturvallisuus käsitteenä esiintyy oikeustieteessä. Haen vastausta myös siihen, millaisen roolin tietoturvallisuus saa osana hyvän hallinnon säännöstöä viranomaisen omassa toiminnassa ja hallinnon palveluita käyttävän näkökulmasta sekä minkälaisia mahdollisia perustuslaillisia ulottuvuuksia tietoturvallisuudella on. Tutkimus käsittelee tällöin yhteiskunnallisen muutoksen ja oikeuden välisen vuorovaikutuksen analysointia oikeustieteen näkökulmasta. Edellä mainittujen kysymysten pohjalta muodostan tutkimuskysymykseni seuraavasti:

1. Miten kansallinen lainsäädäntö velvoittaa viranomaista huolehtimaan tietoturvallisuudesta sekä mistä tietoturvallisuus oikeudellisena käsitteenä koostuu?
2. Millaisen käsitesisällön sekä roolin tietoturvallisuus saa osana hyvän hallinnon tunnusmerkistöä sekä laajemmin mahdollisena perusoikeutena?

Etsiessä vastausta molempiin tutkimuskysymyksiin tutkielma rajataan koskemaan pääsääntöisesti kansallista [13] lainsäädäntöä. Tutkielmassa käsitellään nimenomaan

[13] Tutkielmassa on kuitenkin viittauksia säädöskokonaisuuksiin, joilla on implementoitu EU-asetuksia osaksi kansallista lakia.

tietoturvallisuutta, jota ei tule sekoittaa tietosuojan[14] kanssa. Tietoturvallisuus on vain yksi keino suojata henkilötietoja, johon liittyy tietoturvasääntelystä eriäviä periaatteita ja säännöksiä[15]. Lähestyn tutkimuksen tietoturvallisuutta koskevaa osiota Pöystiä[16] mukaillen niiden tietoturvallisuusominaisuuksien[17] kautta.

Hahmotan tietoturvallisuuden käsitesisältöä osana hyvää hallintoa sen perustuslain (731/1999, PeL) 21 §:n ja hallintolain (434/2003, HaL) 2 luvun tunnusmerkistön kautta. Tässä keskeisenä ovat etenkin perustuslain 12 §:n 2 momentti julkisuuden osalta sekä hallintolain 7 §:n palveluperiaatteen osalta. Tietoturvallisuuden perusoikeudellisia tunnusmerkistöjä lähestyn perustuslain 22 §:n julkisen vallan perusoikeuksien turvaamisvelvoitteen kautta. Rajauksella tietoturvallisuuden rooli osana hyvän hallinnon säännöstöä kattaa niin viranomaisen sisäisen toiminnan, hallinnon asiakkaan ja hallinnon välisen suhteen sekä yleisen velvoitteen huolehtia tietoturvallisuudesta.

Tutkimukseni tutkimussuuntaus sijoittuu lainoppiin, eli oikeusdogmatiikkaan. Lainoppi luo normatiivista tietoa voimassa olevien oikeusnormien todellisuudesta. Lainopin tehtäväksi oikeuskirjallisuudessa yleisen käytännön[18] mukaisesti nähdään olevan oikeusnormien tulkinta ja systematisointi.[19] Lainoppi on oikeustieteen metodeista vanhin sekä käytännön kannalta tärkeimpiä[20]. Lainoppi tutkii siis tarkemmin voimassa olevaa oikeutta ja sitä, minkälaisen merkityksen se saa kirjoitetusta laista sekä muista oikeuslähteistä[21]. Siltala (2003) käsittää lainopin tuottavan perusteltuja oikeuslauseita. Oikeuslauseet ovat oikeudellisia systematisointi ja tulkintakannanottoja voimassa olevan oikeuden säännöistä sekä punnintakannanottoja oikeusperiaatteista.[22]

---

[14] Tietosuojalla tarkoitetaan nimenomaisesti henkilötietojen käsittelyyn ja suojaamiseen liittyvää toimintaa.
[15] LVM/2021/44, s. 4
[16] Pöysti ja muut, 1997. S.58 Pöysti näkee tietoturvallisuusominaisuudet (saatavuus, eheys ja luottamuksellisuus) tietoturvallisuuden oikeudellisen arvioinnin lähtökohtana
[17] Ks. tietoturvallisuusominaisuuksista s. 23-25
[18] Ks. Aarnio, 2006. s. 238
[19] Hirvonen, 2011, s. 22
[20] Aarnio, 2006. s. 238
[21] Hirvonen, 2011, s. 23.
[22] Siltala, 2003, s. 109

Lainoppi jakautuu yleisesti käytännölliseen ja teoreettiseen lainoppiin. Käytännöllisen lainopin keskiössä on oikeuden sisällön tulkitseminen sekä oikeusperiaatteiden punninta [23]. Teoreettisessa lainopissa systematisoidaan oikeudenalakohtaisia yleisiä oppeja tutkimalla ja jäsentämällä oikeudenalojen käsitteitä, oikeusperiaatteita ja teoreettisia rakennelmia [24]. Käytännöllisen ja teoreettisen lainopin liian voimakas erottelu ei kuitenkaan ole tarpeen, sillä ne ovat vuorovaikutussuhteessa toisiinsa[25]. Tämä tutkielma voidaan kuitenkin nähdä asettuvan lainopin käytännölliseen puoleen.

1.2.1.1 Oikeuslähdeopista

Oikeuslähteet ovat jaoteltu suomalaisessa oikeuskirjallisuudessa perinteisesti vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin [26]. Aarnion klassinen hahmotelma on kuitenkin yli 30 vuotta vanha, jonka aikana suomalainen oikeusjärjestys on kokenut varsin suuria muutoksi. Myöhemmin Aarnio onkin päivittänyt omaa oikeuslähdeopillista käsitystään lisäämällä siihen kuuluvaksi myös kielletyt oikeuslähteet sekä EU tasoisen sääntelyn.[27]

Aarnio käsittää vahvasti velvoittaviin oikeuslähteisiin kuuluvan kansallisen oikeuden ulkopuolisista normeista Eurooppaoikeuden sitovat osat, Euroopan ihmisoikeussopimuksen normit, EU-tuomioistuimen sekä Euroopan Ihmisoikeustuomioistuimen tietyt ennakkopäätökset ja systeemiperusteet. Kansallisen oikeuden vahvasti velvoittaviin oikeuslähteisiin kuuluvat perustuslaista johdettavat perusoikeudet, lait ja niiden nojalla annetut alemman asteiset normit, kansainväliset sopimukset jotka on liitetty osaksi kansallista oikeutta sekä maantapa. [28] Vahvan oikeuslähteen ohittaminen tekee ratkaisusta lainvastaisen, jolloin tulkinta tulee kumota

[23] Tuori 2000, s.303.
[24] Hirvonen, 2011, s. 25
[25] Hirvonen, 2011, s. 25
[26] Aarnio, 1989, s. 220
[27] Aarnio, 2006, s. 292
[28] Aarnio, 2006, s. 292

muutoksenhaussa. Vahvasti velvoittavan oikeuslähteen soveltaminen on näin ollen pakollista[29].

Heikosti velvoittaviin oikeuslähteisiin kuuluvat lainsäätäjän tarkoitus ja ennakkoratkaisut[30]. Heikosti velvoittavan oikeuslähteen soveltaminen ei ole pakollista, tosin päätös voi muuttua tällöin kuitenkin ylemmässä asteessa sen ollessa ristiriidassa ylempien tuomioistuinten ennakkoratkaisujen kanssa. Lainsäätäjän tarkoitusta pohdittaessa on kysymys historiallisesta tarkoituksesta, joka on ollut säädöksen säätämisen perusteena, jonka edistämistä säädöksen on katsottu varmistaman [31] . Lainsäätäjän tarkoitusta voidaan hahmottaa erinäisten lain esitöiden, kuten komiteamietintöjen, hallituksen esitysten eduskunnalle ja eduskunnan valiokuntien mietintöjen kautta. Muistisääntönä voidaan pitää sitä, mitä lähempänä oikeuslähde on eduskunnan päätöksentekoa, sitä enemmän painoarvoa sille voidaan antaa tulkittaessa lainsäätäjän tarkoitusta. Tällöin hallituksen esityksillä on varsin merkittävä painoarvo, mikäli esitystä ei ole muutettu eduskunnassa.[32]

Sallittuihin oikeuslähteisiin lukeutuu käytännölliset (taloudelliset, historialliset ja yhteiskunnalliset) argumentit, eettiset ja moraaliset perusteet, yleiset oikeusperiaatteet, oikeustiede ja vertailevat argumentit[33]. Sallittujen oikeuslähteiden sivuuttamisella ei ole ennakoitavia seurauksia, vaan niillä pikemminkin vahvistetaan argumentaatiota. [34] Kiellettyihin oikeuslähteisiin kuuluvat lain ja hyvän tavan vastaiset sekä avoimesti puoluepoliittiset argumentit[35].

[29] Aarnio, 1989, s. 220
[30] Aarnio, 2006, s. 292
[31] Aarnio, 2006, s. 299
[32] Aarnio, 1989, s. 226-227
[33] Aarnio, 2006, s.293
[34] Aarnio, 1989, s. 221
[35] Aarnio, 2006, s. 293

1.3 Oikeusinformatiikka

Tutkielma voidaan jossain määrin asettaa julkisoikeuden, tarkemmin hallinto-oikeuden alaan etenkin hyvää hallintoa ja julkishallintoa käsittelevän teeman perusteella. Viranomaisen toiminnan ja hyvän hallinnon tarkastelu tietoturvallisuuden ja laajemmin digitalisaation kautta näen, että on aiheellisempaa käsittää tutkimus osaksi oikeusinformatiikan alaa.

Oikeusinformatiikka on oikeustieteellinen tutkimus- ja opetusala, jonka tutkimus keskittyy oikeuden ja informaation sekä oikeuden ja tietotekniikan välisiin suhteisiin niiden eri muodoissaan sekä myös niissä ilmeneviin sääntely- ja tulkintakysymyksiin. Oikeusinformatiikka tieteenalana on oikeustieteen sisällä, että sen rajat ylittäen monitieteinen.[36] Yli oikeustieteen rajojen oikeusinformatiikalla on vahvat yhteydet erityisesti tietotekniikkaan, tietojenkäsittelyyn ja yleisesti informaatiotieteisiin. Informaatiohallinnon[37] nopea kehitys on myös liittänyt hallintotieteet ja oikeustieteet väistämättä yhteen uudella tavalla.[38]

Yleisesti oikeusinformatiikka käsitetään kuuluvaksi oikeuden yleistieteisiin [39] . Oikeusinformatiikka on paljolti oikeusteoriaa, mutta se lähestyy näkökulma-avoimena myös konkreettisempia oikeuden ja informaation sekä tietotekniikan välisiin suhteisiin liittyviä kysymyksiä. Tällöin oikeusinformatiikalla on myös yhteyksiä lainoppiin [40] . Toisaalta alati oikeudellistuvassa verkkoyhteiskunnassa oikeusinformatiikka käsittelee myös sellaisia sääntely- ja tulkintakysymyksiä, jotka ulottuvat samalla useille perinteisille oikeustieteen aloille [41] . Oikeusinformatiikan tyypillisiä tutkimusaiheita ovat riskien

[36] Saarenpää & Riekkinen, 2023, s. 21 on todennut oikeusinformatiikan tieteidenvälisyyden korostamisesta tulleen jopa ”hokemanomainen toteamus alan kuvailussa”.
Saarenpää & Riekkinen, 2023, s. 19, s.46: Informaatiohallinnolla Saarenpää kuvaa hallinnon sähköistymistä, jolloin se on tullut riippuvaiseksi tietotekniikasta, tietojärjestelmistä, tietoverkoista ja yleisemmin niiden mahdollistamasta informaatiosta ja viestinnästä.
[38] Saarenpää & Riekkinen, 2023, s. 22
[39] Pöysti, 1999, s. 358
[40] Pöysti, 1999, s. 358
[41] Saarenpää & Riekkinen, 2023, s. 12

tunnistaminen, lainsäädännön muutostarpeen, informaation yhteiskunnallisen merkityksen, tietojärjestelmien ja tietoverkkojen käyttömahdollisuuksien sekä oikeudellisten tietovarantojen ja niiden käytön tutkimus.[42]

Oikeusinformatiikan tavoitteita lainopillisesta näkökulmasta voidaan nähdä olevan normikokonaisuuksien jäsentäminen ja näiden oikeudellisen tulkinnan vahvistaminen niin, että kansalaisten oikeus tietoon sen rajoituksineen tarkentuu. Lainopin normatiivisessa tehtävässään oikeusinformatiikan kannalta ei ole merkitystä, mihin oikeudenalaan säännöksen säätämä normi sijoittuu. Oikeusinformatiikan käytännöllisen lainopin tutkimuksella voidaan tuottaa sellaisia lainsäädännön kehityssuosituksia, joilla voidaan vahvistaa avoimuutta sekä kansalaisten ja yritysten oikeutta tietoon ja tietoturvaan.[43]

Oikeusinformatiikka voidaan jakaa yleiseen ja erityiseen osaan. Yleinen osa käsittelee oikeuden, etenkin ihmisen oikeuksien ja yhteiskunnan suhteen arviointia muuttuvassa yhteiskunnassa. Oikeusinformatiikan erityinen osa koostuu neljästä toisistaan poikkeavasta tutkimus- ja opetusalasta; oikeudellisesta tietojenkäsittelystä, oikeudellisen informaation tutkimuksesta, informaatio-oikeudesta ja tietotekniikkaoikeudesta.[44]

Tutkielmani sijoittuu edellä mainituista tarkemmin informaatio-oikeuden tutkimusalaan. Informaatio-oikeus on suhteellisen uusi ja tuntematon oikeudenala Suomessa, jolla on juurensa 1980-luvulle omana kokonaisuutenaan osana suomalaista oikeusjärjestelmää.[45] Informaatio-oikeus edustaa selkeimmin lainoppiin suuntautuneita lähestymistapoja[46], mikä myötäilee myös tutkielman lainopillista otetta.

---

[42] Saarenpää & Riekkinen, 2023, s. 35
[43] Turunen, 2018, s. 12
[44] Saarenpää & Riekkinen, 2023, s. 36–37
[45] Voutilainen, 2019, s. 21
[46] Pöysti, 1999, s. 363

Informaatio-oikeus voidaan käsittää oikeudenalaksi, joka tutkii informaation tuottamisen, käsittelyn, välittämisen, markkinoinnin, suojaamisen ja säilyttämisen oikeudellista sääntelyä sekä sääntelyn tarvetta ja mahdollisuuksia. Suppeammassa näkökulmassa se on nähty oikeudenalana, joka tarkastelee yksityisyyttä, julkisuutta, televiestintää, informaation vapautta sekä tietoturvaa.[47] Informaatio-oikeuden sisällöstä on tosin esitetty useita erinäisiä määritelmiä[48].

1.4 Aineisto

Tutkielman kannalta haasteeksi on osoittautunut suomalaisen oikeusinformatiikkaa käsittelevän oikeuskirjallisuuden saatavuus sekä aineiston ajantasaisuus. Tutkielman keskeisenä lähteenä teoreettisen osion kannalta on toiminut Ahti Saarenpään ja Juhana Riekkisen teos Oikeusinformatiikan perusteet. Kyseinen teos ansaitsee erityismaininnan kattavuudeltaan, ajantasaisuudeltaan sekä saatavuudeltaan [49] tehden siitä poikkeuksellisen teoksen kansallisessa oikeusinformatiikkaa käsittelevässä kirjallisuudessa. Myös Ahti Saarenpään muita teoksia hänen laajasta tuotannostaan on käytetty olennaisesti. Tutkielmassa olen hyödyntänyt myös Valtiovarainministeriön ja Lapin yliopiston oikeusinformatiikan instituutin toteuttamaa tietoturvallisuuden oikeudellista sääntelyä käsittelevää asiantuntijaselvitystä tietoturvallisuus ja laki. Lisäksi tutkielmassa on hyödynnetty laajasti myös Tomi Voutilaisen laaja-alaista tuotantoa liittyen hallinnon digitalisaatioon.

Tutkielman aiheiden kannalta keskeinen kirjallisuus on jäsenneltävissä pääpiirteittäin kolmeen eri aihepiiriin. Ensimmäiseen aihepiiriin lukeutuu kirjallisuus, jonka kautta käsittelen tutkielman kannalta keskeisiä metodeja, oikeuslähdeoppia ja oikeusinformatiikkaa. Tästä keskeisiä ovat erityisesti edesmenneen Aulis Aarnion kirjallisuus metodien ja oikeuslähdeopin osalta. Toiseen aihepiiriin lukeutuu hyvää

[47] Korhonen, 2006, s. 92.
[48] Ks. Korhonen 2006, s. 94-98 kattava listaus eri tutkijoiden tulkinnoista.
[49] Saarenpään ja Riekkisen teos oikeusinformatiikan perusteet on vapaasti saatavilla Lapin yliopiston Lauda palvelussa.

hallintoa käsittelevä kirjallisuus, jota jäsennän erityisesti Kauko Heurun, Ida Koiviston, Olli Mäenpään ja Heikki Kullan tuotannon kautta. Lisäksi sähköisen hyvän hallinnon osalta olen käyttänyt Tomi Voutilaisen väitöskirjaa Hyvä sähköinen hallinto, joka on toiminut myös tämän tutkielman innoittajana.

Kolmanteen aihepiiriin sisältyy tietoturvallisuuden säätely. Tietoturvallisuuden vallitsevaa lainsäädäntöä ja oikeuskäytäntöä pohjustaessa olen tukeutunut pääosin lainvalmisteluaineistoon etenkin hallituksen esityksien kautta sekä viranomaisen tietoturvallisuudesta vastaavien organisaatioiden viranomaisjulkaisuihin.

1.5 Rakenne

Toisessa luvussa hahmotan oikeusperiaatteiden asemaa oikeustieteen sisällä sekä tietoturvallisuusperiaatteen ja tietoturvallisuuden käsitteen sisältöä. Kolmannessa luvussa käsittelen viranomaisen lainsäädännöllisiä edellytyksiä tietoturvan edistämiseksi. Toisen ja kolmannen luvun kautta vastataan etenkin ensimmäiseen tutkimuskysymykseen. Neljännessä luvussa käsittelen hyvän hallinon ja sähköisen hallinnon käsitettä ja tunnusmerkistöä. Viidennessä luvussa pyrin hahmottamaan hyvän hallinnon ja tietoturvallisuuden yhteyksiä sekä tietoturvallisuuden roolia osana hyvää hallintoa vastaten tutkielman toiseen tutkimuskysymykseen.

2 Tietoturvallisuus oikeusperiaatteena

Tutkielman käsitellessä paljon erinäisiä oikeusperiaatteita on syytä tarkentaa mitä oikeusperiaatteilla tarkoitetaan niillä ollessa varsin keskeinen rooli tutkielman ja 2000-luvun suomalaisen oikeusjärjestyksen sekä oikeustieteellisen kirjallisuuden parissa. Oikeusperiaatteille ei ole suomalaisessa oikeusajattelussa annettu tyhjentävää määritelmää, vaan niitä kuvastaakin varsin moninainen merkityssisältö. Jo pelkästään hallinto-oikeudessa sekä sitä käsittelevässä julkisoikeudellisessa oikeuskirjallisuudessa on löydettävissä satoja erilaisia oikeusperiaatteita[50]. Oikeusperiaatteita onkin kuvattu oikeudellisessa ajattelussa varsin erityislaatuisena ilmiöinä, sillä niihin vedotaan usein jopa itsestäänselvyytenä niiden sisällön ollessa luonteeltaan kuitenkin varsin häilyvä[51].

Suomalaisessa oikeusteoreettisessa kirjallisuudessa on ollut varsin kattavaa keskustelua oikeusperiaatteista viime vuosikymmenien aikana. Keskustelu on painottunut erityisesti oikeudellisten sääntöjen sekä periaatteiden välisestä rajanvedosta, sekä niiden erottelun merkityksestä. Tätä keskustelua on pohjustanut keskeisesti Roland Dworkinin ajatukset oikeusperiaatteiden roolista oikeusnormeina perinteisten sääntöjen rinnalla. Suomalaisessa oikeusteoreettisessa keskustelussa sääntöjen ja periaatteiden suhde näyttäytyy yhtenä keskeisimpänä oikeusteoreettisena ongelmana.

Dworkin näkee oikeusperiaatteiden ja oikeussääntöjen yhden keskeisen eron olevan siinä, että periaatteiden olemassaoloa ei voida johtaa H.L.A. Hartin alun perin esittämän tunnistamissäännön (rule of recognition) kautta, vaan niiden oikeudellinen sisältö määrittyy niihin kohdistuvasta institutionaalisesta tuesta (institutional support) laissa, sen esitöissä sekä julkisesta tuesta. Oikeusperiaatteiden velvoittavuutta määrittelee tällöin sille löydettävän institutionaalisen tuen määrä (weight).[52] Alexy (2000) on

[50] Tähti, 1995, s.527–534.
[51] Tähti, 1999, s.2.
[52] Dworkin, 1977, s.40

hahmottanut oikeusperiaatteet tietynlaisina optimointikäskyinä joita voidaan soveltaa eriasteisesti[53].

Sääntöjen ja periaatteiden väliset erot esiintyvätkin tarkemmin etenkin niiden välisessä ristiriitatilanteessa. Sääntöjen ristiriita voidaan ratkaista yleisesti metanormien avulla. Tällaisia metanormeja ovat esimerkiksi ylemmänasteinen normi syrjäyttää alemmanasteisen (lex superior derogat legi inferiori), erityislaki syrjäyttää yleislain (lex specialis derogat legi generali) ja myöhempi laki syrjäyttää aikaisemman lain (lex posterior derogat legi priori).[54] Kun taasen oikeusperiaatteet ovat ristiriidassa keskenään, niiden väliset suhteet voidaan ratkaista periaatepunninnan avulla. Tällöin arvioidaan eri periaatteiden painoarvoa ja punnitaan niiden merkityksiä kyseisen tilanteen mukaisesti. [55] Tilanteessa missä yksi periaate asetetaan etusijalle toiseen nähden, sovelletaan sen periaatteen oikeudellista vaikutusta joka punnitaan painavammaksi.[56]

Dworkinin ja Alexyn ajatuksia mukaillen Tolonen (2008) on tiivistänyt oikeusperiaatteiden ja sääntöjen eroavan toisistaan kolmessa eri suhteessa tunnistamisehtojen, soveltamisehtojen ja ristiriitatilanteiden kautta. Tunnistamisehdossa säännöt johdetaan tunnistamissäännön kautta. Periaatteet voidaan tunnistaa niiden saaman institutionaalisen tuen kautta, jota ei voida mitata niinkään formaalisin[57] kriteerein. Toisena erona Tolonen esittää soveltamisehdot, jossa säännöt nähdään ”joko-tai-soveltamisena”. Sääntöjä näin ollen sovelletaan sellaisenaan, tai ollaan soveltamatta. Periaatteen tunnistamisehdot kumpuavat sen painon, arvon ja sovellustilanteen olosuhteiden - institutionaalisen tuen mukaan. Kolmantena sääntöjen ja periaatteiden erona Tolonen mainitsee niiden ristiriitatilanteet. Sääntöjen ristiriitatilanteet ovat ratkaistavissa oikeusjärjestyksen formaalien kriteereiden kuten lex superior, lex posterior ja lex specialis derogat legi generali avulla. Periaatteiden

[53] Alexy, 2000, s.295. Lähde: Ratio Juris. Vol. 13 No. 3 September 2000,
[54] Pöysti, 1999. s.113. ks. lisää metanormeista Tuori 2000, s. 184-185.
[55] Alexy, 2000, s. 298
[56] Alexy, 2000, s. 297
[57] Tolonen, 2008, s.XII, XIX. Formaalilla Tolonen tarkoitti tuotannossaan muodollista, lainsäädäntöä painottavaa lain tulkintaa.

ristiriitatilannetta ei ole mahdollista ratkaista formaalien kriteerien avulla, vaan niiden päällekkäisyys on ratkaistava niiden merkityksen ja arvon mukaan, mikä niille toisiinsa nähden sovellutustilanteessa annetaan.[58] Useiden erilaisten oikeusperiaatteiden määrä ja niiden ilmeneminen eri oikeudenaloilla tekee niiden välisestä tulkinnasta varsin vaikeaa. Oikeustieteessä ei ole löydettävissä tyhjentävää luetteloa tunnetumpien, kuten oikeusvaltioperiaatteen sekä vähemmän tunnettujen oikeusperiaatteiden, kuten tietoturvallisuuden periaatteen välisestä suhteesta niin, että niiden välille voitaisiin luoda jonkinlainen hierarkia joka erottaisi varsinaiset ja epävarsinaiset periaatteet. Näin ollen ei oikeusperiaatteiden poissuljentaa voida suorittaa, varsinkin jos niiden merkityssisältöä pyritään hahmottamaan oikeuskirjallisuuden, lain esitöiden tai laillisuusvalvojien päätöksien kautta. Tähti näkee ongelman ytimen olevankin oikeusteorian tavassa asennoitua periaatteita kohtaan kuin ne olisivat yhtenäinen kokonaisuus, vaikka reaalimaailmassa näin ei ole.[59]

Oikeusperiaatteiden monitulkintaisuus korostuu erityisesti niiden runsaassa määrässä ja niiden ilmenemisessä eri oikeudenaloilla. Tyhjentävää luetteloa tunnetuista oikeusperiaatteista ei ole mitenkään mahdollista, saati edes tarkoituksenmukaista luoda vaikuttaen niiden väliseen punnintaa entisestään. Oikeusperiaatteiden keskiössä näyttää olevan institutionaalisen tuen käsite, joka antaa sille oikeudellisessa punnintatilanteessa painoarvoa. Institutionaalisen tuen määrää voidaan johtaa lainsäädännöstä sekä julkisesta tuesta. Tämä oikeusperiaatteiden monimutkainen luonne vaatiikin jatkuvaa keskustelua, systematisointia ja punnintaa oikeustieteen sisällä.

2.1 Tietoturvallisuuden periaatteesta

Tietoturvallisuutta voidaan tarkastella useista eri näkökulmista, jolloin tietoturvallisuuden periaate ilmenee eri oikeudenaloilla vaihtelevalla sisällöllä [60] . Tutkielman tutkimussuuntauksen kannalta on syytä keskittyä sen ilmenemiseen

[58] Tolonen, 2008, s.50-53
[59] Tähti, 1999, s. 2
[60] Voutilainen, 2009, s. 196

informaatio-oikeuden näkökulmasta. Informaatio-oikeudessa tietoturvallisuuden periaate ilmenee yleisenä periaatteena oikeutena tietoturvaan[61].

Tietoturvallisuus oikeusperiaatteena kokoaa systemaattisesti alleen ne normit, jotka käsittelevät informaation, tietojenkäsittelyn ja tietoliikenteen saatavuuden, eheyden ja luottamuksellisuuden ylläpitämistä sekä suojaamista. Tietoturvallisuuden normisto asettaakin tällöin välittömiä ja välillisiä velvoitteita viranomaiselle edistää saatavuuden, eheyden ja luottamuksellisuuden suojaavia toimenpiteitä. [62] Voutilainen (2009) on kuvannut tietoturvallisuuden keskeisiksi suojaamiskohteiksi viranomaistoiminnassa tietojenkäsittelytoiminnot, julkisuuden, salassapidon ja tietosuojan[63].

Tietoturvallisuutta on kuvattu myös hiljaisena periaatteena. Hiljaisella periaatteella tarkoitetaan tietoturvallisuuden osalta sitä, että se on ollut suojattava oikeushyvä lukuisissa vanhoissa oikeussäännöissä ilman, että tietoturvallisuus ilmenisi itsenäisenä oikeudellisena käsiteenä. Nykyisessä oikeudellisessa digitaalisessa verkkoyhteiskunnassa tietoturvallisuuden oikeusperiaate on kuitenkin noussut itsenäiseksi oikeusperiaatteeksi, jolloin tietoturvallisuudesta kannetaan avoimesti ja näkyvästi huolta. Tietoturvallisuus käsitetäänkin verkkoyhteiskunnan eräänä keskeisimpänä metaoikeutena. [64] Metaoikeuksilla tarkoitetaan yhteiskuntasopimuksen tasoisia tavoitteellisia ja moraalisia päämääräoikeuksia, joista ei sellaisinaan ole nimenomaisia perusoikeustasoisia säännöksiä, mutta ne ovat perus- ja ihmisoikeuksien sääntelyn toteuttamisen keskeisiä edellytyksiä.[65] Metaoikeudet auttavat tiivistämään erilaisia näkökulmia ja vaatimuksia, joita on otettava huomioon kohdattaessa teknologian ja oikeuden välisiä oikeudellisia ongelmia[66].

[61] Saarenpää & Riekkinen, 2023, s. 172
[62] Pöysti, 1999, s. 454
[63] Voutilainen, 2009, s. 198
[64] Pöysti, 2002, s. 59-61
[65] Saarenpää & Riekkinen, 2023, s. 172
[66] Pöysti, 2002, s. 42

2.2 Tietoturvallisuuden käsitteestä

Tietoturvallisuuden tutkimus on lähtökohtaisesti varsin moni- ja poikkitieteellisetä. Vaikka tämä pro -gradu tutkielma on tutkimusotteeltaan lainopillinen, koen tarpeelliseksi myös pohtia tietoturvallisuuden termin ilmenemistä oikeustieteen ulkopuolella. Tällöin myös tietoturvallisuuden hahmottaminen oikeustieteellisenä ilmiönä selkeentyy. Yleisesti tietoturvallisuus saatetaan mieltää tietotekniikkaan, vaikka tietoturvallisuutta käsittelevien tieteenalojen kirjo on varsin laaja.

Saarenpää näkee tietoturvallisuuden turvallisuuden muotona, joka on vaihtanut muotoaan ja nimikettään pitkän historiansa aikana. Yleisesti tietoturvallisuutta on mahdollista tarkastella useiden eri näkökulmien ja historiallisten lähtökohtien kautta.[67] Tietoturvallisuus saatetaankin nykyään käsittää helposti osaksi digitaalista toimintaa, vaikka tietojen suojaamista onkin toteutettu erinäisten toimenpiteiden avulla tuhansia vuosia. Valtiovarainministeriön julkisen hallinnon digitallista turvallisuutta käsittelevässä julkaisussa tietoturvallisuus nähdään osana digitaalisen turvallisuuden viitekehystä. Digitaalisen turvallisuuden termi on kuitenkin varsin uusi eikä ole vakiintunut kansallisesti tai kansainvälisesti.[68]

Yleisessä kielenkäytössä tietoturvallisuus ja tietoturva nähdään synonyymeina, joilla tarkoitetaan tiedon ominaisuuksien hallintaa, tiedon laadun säilyttämistä ja tietojenkäsittelyn turvaamista. Tarkemmin tarkasteltuna niiden välillä voidaan kuitenkin nähdä eroja, missä tietoturva pitää sisällään hallinnolliset ja tekniset toimet tietoaineistojen suojaamiseksi ja tietoturvallisuus taasen tarkoittaa tilaa, mihin pyritään tietoturvatoimia toteuttamalla.[69] Tietoturvallisuuden käsiteestä onkin esitetty useita erilaisia määrittelyitä, jotka vaihtelevat sen mukaan, minkä osa-alueen kautta tietoturvallisuutta tarkastellaan[70].

[67] Saarenpää & Riekkinen, 2023, s. 198
[68] VM 2020:23, s. 16
[69] Voutilainen, 2009, s. 198
[70] VAHTI 2/2004, s. 15

2.2.1 Tietoturvallisuuden osa-alueet

Yleisen käytännön mukaan tietoturvallisuus jaotellaan kahdeksaan eri osa-alueeseen: hallinnolliseen tietoturvallisuuteen, henkilöstöturvallisuuteen, fyysiseen turvallisuuteen, tietoliikenneturvallisuuteen, laitteistoturvallisuuteen, ohjelmistoturvallisuuteen, tietoaineistoturvallisuuteen ja käyttöturvallisuuteen.[71]

Hallinnollinen tietoturvallisuus koostuu organisaation tiedonhallintayksikön laatimasta tietoturvallisuuspolitiikasta, joka pitää sisällään organisaation toimintalinjaukset, periaatteet, organisaatiojärjestelyt, henkilöstön tehtävät ja vastuualueet sekä ohjeistuksen, koulutuksen ja valvonnan tietoturvallisen toiminnan edistämiseksi[72].
Henkilöstöturvallisuus tarkoittaa henkilöstöstä aiheutuvien riskien hallintaa. Jopa puolet kaikista tietoturvarikkomuksista liittyy organisaation menettelytapoihin. [73] Henkilöstöturvallisuutta toteutetaan soveltuvuuden, toimenkuvien sekä tiedonsaanti- ja käyttöoikeuksien avulla [74] . Fyysinen turvallisuus on organisaatioiden häiriöttömän toiminnan turvaamista kaikissa olosuhteissa, ottaen huomioon riskit ja erityistarpeet. Fyysistä turvallisuutta toteutetaan käytännössä erinäisten valvontatoimenpiteiden kuten kulunvalvonnan, kameravalvonnan ja vartioinnin avulla sekä kiinteistön rakenteellisten palo-, vesi- ja ilmastointivahinkojen torjunnalla. [75] Tietoliikenneturvallisuudella tarkoitetaan organisaatioiden tietoliikennetoimintojen turvaamista tietoliikenteeseen kohdistuvien uhkien osalta. Tietoliikenneturvallisuuden alueeseen lukeutuu muun muassa tietoliikennelaitteiston kokoonpano, luettelointi, ylläpito ja testaus, viestinnän salauksen varmistaminen tietoturvallisella tavalla, olennaisten tietoturvapoikkeamien havainnointi ja dokumentointi. [76] Laitteistoturvallisuudella tarkoitetaan laitteistojen käyttöönottoa, ylläpitoa sekä käytöstä poistoon liittyvien toimien hallinnointia, turvaten

[71] Ks. Mm. VAHTI 2/2004. s. 15–16, VM 2000:11. s. 8, Andreasson & Koivisto. 2013. s. 52
[72] VM 2000:11, s. 8
[73] VAHTI 2/2008, s. 11–12
[74] VM 2000:11, s. 8
[75] VAHTI 3/2007, s. 59
[76] VAHTI 3/2007. s. 61

laitteisto koko elinkaaren ajalta. [77] Ohjelmistoturvallisuudella tarkoitetaan kaikkea tietojenkäsittelyn ja tietoliikennetekniikan liittyvien ohjelmistojen turvallisuuden liittyviä tietoturvallisuustoimenpiteitä, pitäen sisällään ohjelmistot, valvonta- ja lokimenettelyn sekä ohjelmistojen päivittämisen ja ylläpidon. [78] Tietoaineistoturvallisuus käsittelee tietojen suojausta tiedon kaikissa talletusmuodoissa. Tietoaineistojen turvallisuuden varmistamiseksi on tiedonhallintayksikön laadittava organisaatiokohtaiset ohjeet, jotka koskevat koko henkilöstöä tietoaineistojen koko elinkaaren ajalta. [79] Käyttöturvallisuudella tarkoitetaan tietotekniikan turvallisen käytön toimintaolosuhteiden edellytyksiä sekä niiden luomista ja ylläpitoa. Käytännössä käyttöturvallisuus ilmenee muun muassa tietojärjestelmien suojaamisella haittaohjelmilta sekä varmuuskopioinnilla.[80]

Tietoturvallisuus tuleekin nähdä laajana ja monitahoisena käsiteenä, missä jokainen näistä osa-alueista edellyttää erilaisia toimenpiteitä ja suunnitelmia tietoturvallisuuden varmistamiseksi organisaation toiminnassa. Yhdessä ne muodostavat kokonaisvaltaisen lähestymistavan tietoturvallisuuteen, joka pyrkii suojaamaan organisaation tietoja ja toimintaa eri uhkia vastaan. Lisäksi tietoturvallisuuden osa-alueet on nähty olevan etenkin lain esitöissä yksittäisten tietoturvallisuussäännösten sääntelykohteena.

2.3 Tietoturvallisuudesta oikeustieteellisenä käsitteenä

Voutilainen (2009) käsittää oikeudellisesta näkökulmasta tietoturvan ja tietoturvallisuuden käsitteillä eron, missä tietoturva ilmenee oikeuskäsitteenä ja tietoturvallisuus oikeusperiaatteena[81]. Kansallisessa laissa tietoturvallisuudesta esiintyy kahdenlaisia määritelmiä. Laissa sähköisen viestinnän palveluista (917/2014, SVPL) tietoturvalla tarkoitetaan

[77] VAHTI 3/2007. s. 63
[78] VAHTI 3/2007. s. 69
[79] VAHTI 3/2007. s. 55
[80] VAHTI 3/2007. s. 65
[81] Voutilainen, 2009. s. 199

”*hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (SVPL 3 § kohta 28)”*

Määritelmä eroaa sisällöltään siitä, mitä viranomaisen tietoturvallisuudesta yleislain tasolla säätävässä laissa julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki, TiHL). Tiedonhallintalaissa määritellään tietoturvallisuustoimenpiteen käsite, jolla tarkoitetaan

”tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamisesta hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä (TiHL 2 § 9 kohta).”

SVPL ja tiedonhallintalain määritelmät tietoturvasta ja tietoturvallisuustoimenpiteistä ovat hyvin samankaltaiset tulkittavalta sisällöltään, tosin niiden sanamuodot eroavat toisistaan. Eron niiden välille tekee tiedonhallintalaissa esiintyvät saatavuuden, eheyden ja luottamuksellisuuden käsitteet, sekä maininta toiminnallisista toimenpiteistä.

Tietoturvallisuussääntelyn perusominaisuuksiksi on kirjallisuudessa ja lukuisissa tietoturvallisuusnormistoissa luettu luottamuksellisuus, eheys ja saatavuus. Näillä ominaisuuksilla kuvataan tietoturvallisuustoiminnan päämäärän erinäisiä ulottuvuuksia ja osa-alueita [82] . Pöysti (1997) käsittää informaation ja tietojenkäsittelyn tietoturvallisuusominaisuudet tietoturvallisuuden oikeudellisen arvioinnin lähtökohdaksi. Tietoturvallisuusominaisuudet muodostavat tietoturvallisuusnormeiksi luokiteltavien oikeusnormien tunnistamisen perusteet. Näin ollen, ne luovat myös tietoturvallisuusperiaatteen ja -käsitteen systemaattisen perustan.[83]

[82] Pöysti & Saarenpää, 1997, s. xxxiv ja s. 58
[83] Pöysti & Saarenpää, 1997, s.59

2.3.1 Saatavuus

Tiedon saatavuudella [84] tarkoitetaan vaatimusta siitä, että tiedot ovat vain niihin oikeutettujen saatavilla suunnitellulla tavalla käyttökelpoisessa muodossaan. Näin ollen tiedon käytettävyys koostuu tiedon saatavuudesta ja tiedon käyttökelpoisuudesta. Tiedon käytettävyyden käsite pitää sisällään myös ajalliseen, käyttötarkoitukselliseen ja muotoon liittyvät ulottuvuudet. Tiedon muodolla kuvataan vaatimusta siitä, että tiedon on oltava siinä muodossa, että se on käytettävissä halutulla tietojenkäsittelyvälineellä, kuten tietojenkäsittelyohjelmalla. [85] Viranomaistoiminnassa tiedon käytettävyydestä huolehtinen tarkoittaa, että virkatehtävissä tarvittavat tiedot ovat häiriöttömästi ja toiminnan edellyttämällä tavalla saatavissa. Käytettävyyteen viranomaistoiminnassa liittyy myös muiden viranomaisten tiedontarpeiden huomioiminen, mikäli toinen viranomainen on riippuvainen muualta saatavasta tiedosta.[86] Viranomaisten onkin siis huolehdittava hallussa olevien tietojen saatavuudesta myös teknisten käyttöyhteyksien osalta silloin, kun toinen viranomainen tarvitsee tietoja osana omien tehtäviensä hoitoa[87].

2.3.2 Eheys

Tiedon eheydellä tarkoitetaan tiedon muodon säilyttämistä tahattomalta tai lainvastaiselta muuttamiselta. Tiedon eheydellä kuvataan siis tiedon säilyttämistä tallennettua tietoa verrattavassa muodossa.[88] Sähköisessä toimintaympäristössä tiedon eheyden takaaminen ilmenee monella erinäisellä tavalla, kuten tietojen lähettämisessä tietoverkkojen avulla käyttäen salausmenetelmiä. Tällöin pyritään ensinnäkin tiedon luottamuksellisuuden säilymiseen sekä tiedon alkuperäisen muodon säilymisestä tiedon vastaanottajalle. Osana hallinnollista päätöksentekoa tiedon eheyden tehtävänä on taata päätöksen muuttumattomuus, kun päätös on tehty ja päätöstä koskeva asiakirja on

[84] Kirjallisuudessa tiedon saatavuus esiintyy synonyyminä tiedon käytettävyydelle.
[85] Voutilainen, 2012. s. 118
[86] HE 30/1998 vp, s. 77
[87] Voutilainen, 2012. s. 119
[88] HE 30/1998 vp, s. 77

vahvistettu.[89] Pöysti on liittänyt tiedon eheydelle myös tiedon oikeellisuuden, aitouden ja ajantasaisuuden säilyttämisen tavoitteet sekä kiistämättömyyden, jolloin tiedon laatijan tai lähettäjän jälkikäteinen todentaminen voidaan varmentaa.[90]

2.3.3 Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan informaation ja tietojenkäsittelyn säilymistä vain siihen oikeutettujen käytettävissä. Luottamuksellisuus pitää sisällään informaatioon sisältyvien käyttö- ja määräämisoikeuksien asiallisen sisällön turvaamisen tietoturvatoimenpiteiden avulla, joilla varmistetaan perus- ja ihmisoikeuksien, kuten viestinnän salaisuuden toteutuminen osana tietojenkäsittelyä. Luottamuksellisuus käsittää myös ajallisen ulottuvuuden, eli tiedon käyttöoikeuksien kestosta ja milloin tietojenkäsittelytoimenpiteet ovat sallittuja sekä käyttötarkoitussidonnaisuuden, eli mihin tarkoitukseen tietoja saa käsitellä ja käyttää. [91] Tiedon luottamuksellisuus järjestetään käytännössä niin, että tiedonhallintayksikkö kartoittaa tietovarannot erinäisiin suojausluokkiin sekä määrittelee henkilöstölle tietojenkäsittelyyn liittyvät työtehtävät sen mukaan, kenellä on oikeus käyttää viranomaisen tietovarantoja tiettyyn määriteltyyn tarkoitukseen[92].

Tiedon eheyden, luottamuksellisuuden ja saatavuuden ominaisuuksien turvaaminen ovat toisiinsa kietoutuneita ominaisuuksia, jolloin yhden ominaisuuden laiminlyönti mahdollisesti vaarantaa muiden ominaisuuksien turvaamisen. Tietoturvallisuustoimenpiteitä ei siis tulisi kohdistaa tiettyihin tiedon perusominaisuuksiin, vaan niitä tulee suojella kokonaisuutena.
Hahmottaessa tietoturvallisuutta oikeustieteellisenä käsitteenä se esiintyy varsin moniulotteisena. Tietoturvallisuuden ytimessä näyttäytyy kuitenkin olevan tiedon saatavuuden, eheyden ja luottamuksellisuuden ominaisuudet. Oikeustieteellisenä

[89] Vuotilainen, 2012. s. 119-120
[90] Pöysti, 1999, s. 463
[91] Pöysti, 1999, s. 458-459 ja 463
[92] Voutilainen, 2012, s. 120

käsitteenä niillä on tietoturvallisuuden kannalta erittäin keskeinen asema, sillä tietoturvallisuudesta säädettävillä oikeusnormeilla pyritään suojaamaan juuri tiedon ominaisuuksia hyödyntäen erinäisiä tietoturvallisuustoimenpiteitä.

2.4 Viranomaisen tietoturvallisuusvelvoitteet kansallisessa lainsäädännössä

Julkisen hallinnon tietoturvallisen toiminnan vaatimuksesta säädetään useassa kansallisessa lakikokonaisuudessa[93]. Tietoturvallisuus mainitaan kuitenkin useasti vain käsitteen tasolla vaatimuksena, eikä tietoturvallisuuden sisällöstä säädetä tyhjentävästi. Tämä voi osin johtua tietoturvallisuuden toimintaympäristön jatkuvasta muutoksesta, jolloin lainsäätäjä ei ole halunnut määritellä tietoturvallisen toiminnan vaatimuksia tyhjentävästi, sillä tietoturvavaatimukset muuttuvat jatkuvasti teknisen kehityksen sekä muuttuvan toimintaympäristön mukana [94] . Hahmottaessa viranomaisen tietoturvallisuusvaatimuksia on tutkielman kannalta aiheellista keskittyä erityisesti tiedonhallintalakiin, jossa viranomaisen tietoturvallisuusvaatimuksista säädetään yleislain tasolla.

[93] Tietoturvallisuudesta keskeisesti säädetään muun muassa seuraavissa lakikokonaisuuksissa: perustuslaki (731/1999), laki julkisen hallinnon tiedonhallinnasta (906/2019), laki viranomaisten toiminnan julkisuudesta (621/1999), laki sähköisen viestinnän palveluista (917/2014), laki sähköisestä asioinnista viranomaistoiminnassa (13/2003), tietosuojalaki (1050/2018), laki digitaalisten palveluiden tarjoamisesta (306/2019), arkistolaki (831/1994), valmiuslaki (1552/2011), valtion virkamieslaki (750/1994), laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009), henkilökorttilaki (663/2016), laki yksityisyyden suojasta työelämässä (759/2004), laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (661/2009), laki kansainvälisistä tietoturvavelvoitteista (588/2004), laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015).

[94] HE 60/2018 vp, s. 62

3 Tiedonhallintalaki viranomaisen tietoturvallisuutta sääntelevänä yleislakina

Tiedonhallintalain neljännessä kappaleessa säädetään yleislain tasolla viranomaisen tietoturvallisuuden vaatimuksista sekä tietoturvallisuustoimenpiteistä. Tietoturvallisuustoimenpiteiden tavoitteena on varmistaa tietoturvallisuus hyvän hallintotavan mukaisesti, jonka lähtökohtana on riskien kartoittaminen sekä riskien hallinta[95]. Tietoturvallisuustoimenpiteillä tarkoitetaan myös tietoturvallisuuden osa-alueiden, kuten tietoliikenneturvallisuuden, fyysisen turvallisuuden sekä laitteisto- ja ohjelmistoturvallisuuden varmistavia toimenpiteitä. Tietoturvallisuustoimenpiteet tulee suhteuttaa riskienhallinnan keinoin muun muassa uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.[96] Tietoturvallisuustoimenpiteet ovat olennainen osa tiedonhallintaa, jolla tarkoitetaan tiedonhallintalain 2 §:n 8 kohdan mukaan viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä viranomaisen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tallentamis- tai käsittelytavoista. Tiedonhallintalaissa säädetään niistä hallinnollisista, toiminnallisista ja teknisistä vaatimuksista, jotka viranomaisen tulisi toteuttaa tietoturvallisuuden minimitason varmistamiseksi asiakirjoja ja tietoaineistoja käsitellessä.

Tietoturvallisen toiminnan järjestämistä hallinnollisin toimenpitein tarkoitetaan tietoaineistojen organisointia niin, että tietoaineistoja kyetään käsittelemään julkisuusperiaatetta ja viranomaisten toimintaa sekä turvallisuutta palvelevalla tavalla[97]. Käyttöoikeuksien rajaamista tietyille henkilöille voidaan pitää hallinnollisena tietoturvatoimenpiteenä[98]. Toiminnallisilla tietoturvatoimenpiteillä tarkoitetaan niitä

[95] VM 11/2000, s. 8
[96] HE 284/2018 vp, s. 65-66
[97] HE 284/2018 vp, s. 65
[98] VM 2021/65, s. 55

viranomaisen menettelyitä, jotka varmistavat tietoaineistojen turvallisen käsittelyn osana viranomaistoimintaa[99]. Esimerkiksi viranomaisen laatimat prosessikuvaukset ovat osa toiminnallisia tietoturvallisuustoimenpiteitä [100] . Tekniset toimenpiteet pitävät sisällään ne sopivat tekniset toimenpiteet ja ratkaisut, joiden avulla kyetään varmistamaan tietoaineistojen saatavuus, eheys ja luottamuksellisuus [101] . Teknisiin tietoturvallisuustoimenpiteisiin lukeutuvat esimerkiksi erinäisten palomuurien ja salausmenetelmien avulla toteutetut tietoturvallisuustoimenpiteet[102].

Tiedonhallintalain 12 §:ssä säädetään tietoaineistojen käsittelyyn sidoksissa olevan henkilöturvallisuuden täyttämisen perusteista [103] . Tiedonhallintalain 12 § luo tietoturvallisuuden vähimmäisvaatimuksen sille, että tehtävät, joihin edellytetään henkilöltä erityistä luotettavuutta, on tunnistettu julkisessa hallinnossa [104] . 12 §:n viittaukset turvallisuusselvityslakiin (726/2014) ja yksityisyyden suojaan työelämässä (259/2004) eivät luo viranomaiselle lisää velvollisuuksia. Maininnat ovat sisällytetty pykälään informatiivisina ja merkityksellisinä luodessa sääntelykokonaisuutta henkilöturvallisuudesta ja sen perusteista.[105]

Erityistä luotettavuutta edellyttävien tehtävien tunnistaminen voidaan suorittaa määrittämällä erinäiset tilanteet, jolloin henkilön on käsiteltävä työssään säännöllisesti salassa pidettäviä tietoja tai hän työskentelee tiloissa, jossa henkilön tietoon voi tulla muuten kuin satunnaisesti salassa pidettäviä tietoja[106]. Henkilöille, jotka ovat saamassa valtuutuksia käsitellä tietoaineistoja on henkilöturvallisuuden nimissä tehtävien taustatarkastuksien ja turvallisuusselvitysten tavoitteena on varmistaa kyseisen henkilön sopivuus erityistä luotettavuutta edellyttävään tehtävään [107] . Erityistä luotettavuutta

[99] HE 248/2018 vp, s. 65
[100] VM 2021/65, s. 55
[101] HE 284/2018 vp, s. 65
[102] VM 2021/65. s. 55
[103] HE 284/2018 vp, s. 91
[104] VM 2021:65, s. 10
[105] HE 284/2018 vp, s.91–92
[106] VM 2021:65. s.11
[107] VAHTI 2/2008 s. 21

vaativien tehtävien tunnistaminen organisaation sisällä sekä mahdollisten turvallisuusselvityksien tekeminen on tärkeä osa tietoturvallista toimintaa julkisessa toiminnassa, jonka avulla organisaation tietoturvallisuudesta vastaavat henkilöt ovat tietoisia siitä kenellä on tarve ja oikeudet päästä käsiksi arkaluotoiseen tietoon. Sillä kyetään kartoittamaan etukäteen ne työtehtävät, joissa henkilöllä on mahdollista joko tarkoituksellisesti tai tahattomasti aiheuttaa varsin vakaviakin tietoturvarikkomuksia, jolloin esim. tietoturvallisuuskoulutusta kyetään ohjaamaan sinne missä sitä tarvitaan.

Tiedonhallintalain 13 §:ssä säädetään tietoaineistoturvallisuudesta ja tietojärjestelmäturvallisuudesta. Valtiovarainministeriön suosituskokoelman mukaisesti 13 § luo viranomaiselle vähimmäisvaatimukset koostuen toimintaympäristön tietoturvallisuustilan seuraamisesta (13 § 1 mom.), tietoturvallisuuden varmistamisesta tiedon koko elinkaaren ajalta (13 § 1 mom.), tietoriskien hallinnan ja siihen perustuvien tietoturvatoimien järjestämisen (13 § 1 mom.), tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden varmistamisesta (13 § 2 mom.), julkisuus ja salassapitorakenteen huomioimisen osana tietovarantojen tietorakennetta (13 § 3 mom.) ja hankittavien tietojärjestelmien asianmukaisten tietoturvallisuustoimenpiteiden toteuttamisen (13 § 4 mom.).[108]

Voutilainen on hahmottanut tiedonhallintalain 13 §:n ensimmäisestä momentista kumpuavan neljä tiedonhallintayksikölle kohdistuvaa vaatimusta: aktiivisen seurantavelvollisuuden (toimintaympäristön tietoturvallisuuden tilan seuraaminen), varmistamisvelvollisuuden (tietoaineistojen ja tietojärjestelmien tietoturvallisuuden varmistaminen koko elinkaaren), riskien arviointivelvollisuus (olennaisten riskien tunnistaminen) sekä tietoturvallisuustoimenpiteiden mitoittamisvelvollisuus (riskienhallintaan perustuva tietoturvallisuustoimenpiteiden järjestäminen). [109] Lainsäätäjä on maininnut tiedonhallintalain 13 §:n ensimmäisen momentin muodostavan kokonaisuuden, johon kuuluu riskien arviointi,

[108] VM 2021:65, s. 10
[109] Voutilainen, 2019, s. 330

tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen[110].

13 §:n 1 momentin mukaan tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Olennaisilla riskeillä tarkoitetaan niitä riskejä, jotka voivat haittaavalla tai vahingoittavalla tavalla vaikuttaa viranomaisen tai hallinnon asiakkaan toimintaan.[111]

Toimintaympäristön tietoturvallisuuden tilan määrittelyssä tehdään riskien arvioinnin kannalta keskeiset rajaukset riskien arvioinnin sisällöstä ja tunnistetaan merkittävimmät riippuvuudet. [112] Tiedonhallintayksikön seurantavelvollisuus vaatii tiedonhallintayksikköä seuraamaan toimintaympäristössään tapahtuvia muutoksia ja mitoittamaan tietoturvallisuustoimenpiteet suhteessa toimintaympäristön vaatimuksiin. Tiedonhallintayksikön toimintaympäristö tulee kuvata osana tiedonhallintalain 5 §:n säädettyä tiedonhallintamallia [113] , josta seurantakohteet tietoturvallisuuden tilan arvioimiseksi voidaan tunnistaa. Keskeisiä seurantakohteita ovat tietoverkon, tietojärjestelmien ja tietovarantojen sekä niiden sisältämien tietoaineistojen tietoturvallisuustoimenpiteiden riittävyys. [114] Toimintaympäristön tilaan vaikuttavat muutokset voivat olla peräisin myös tiedonhallintayksikön omasta toiminnasta ja päätöksistä tai ulkoisista tekijöistä, kuten lainsäädännöllisistä muutoksista ja hallitusohjelmasta kumpuavista tavoitteista[115]. Tietoturvallisuuden tilaa voidaan seurata myös hallintakeinojen suorituskykyyn ja vaikuttavuuteen perustuvilla mittareilla, jotka

[110] HE 284/2018 vp, s. 92
[111] HE 284/2018 vp, s. 92
[112] VAHTI 22/2017, s. 19
[113] VM 2020:29, s. 11 - ” Tiedonhallintamalli on kuvaus tiedonhallintayksikössä toimivien viranomaisten tehtävien hoidossa toteutettavasta tiedonhallinnasta.”
[114] Voutilainen, 2019, s. 330
[115] VM 2020:53, s. 13

voivat olla esim. numeerisia raja-arvoja (esim. tietoaineistojen käytettävyys vähintään 99 %) tai vaatimusten mukaisuuden varmistamista (esim. säännöllisesti toteutettavien arviointien ja katselmointien toteuttaminen vuosikellon mukaisesti) [116].

Tiedonhallintalain 13 § velvoittaa tiedonhallintayksikköä mitoittamaan tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Tiedonhallintayksikön tulee arvioida tietoaineistoihin ja tietojärjestelmiin liittyviä riskejä säännöllisesti niiden koko elinkaaren ajan. Osana riskienarviointia on tiedonhallintayksikön tunnistettava ne olennaiset riskit, joilla voi olla mahdollista vaikutusta tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden vaarantumiseen taikka tietojärjestelmän käyttöön ja vikasietoisuuteen.

Riskienarvioinnin tulee olla jatkuvaa toimintaa, jossa arvioidaan muun muassa suunnitelmien toteutumista sekä jo toteutettujen tietoturvatoimenpiteiden vaikuttavuutta. [117] Tietoturvallisuusriskien hallinta on yhteydessä muuhun riskienhallintaan organisaation toiminnassa. Tietoturvallisuusriskien hallintaprosessi kokonaisuudessaan pitää sisällään toimintaympäristön määrittämisen, riskien arvioinnin (koostuen tunnistamisesta, analysoinnista ja merkitysten arvioinnista), riskien käsittelyn, riskien hyväksynnän, riskeistä koskevan viestinnän ja tiedonvaihdon sekä riskien seurannan ja katselmoinnin [118] . Tietoturvallisuusriskien hallinnan avulla pyritään varmistamaan tietoturvallisuustoimenpiteiden riittävyys, jotta tietojen luottamuksellisuus, eheys ja saatavuus voidaan suojata. [119] Tietoriskien hallinnalla pyritään saavuttamaan tietoturvallisuustoimenpiteiden yhdentymä, joka mahdollistaa tietoaineistojen ja tietojärjestelmien hyvän tason sekä muodostaa tasapainon käyttäjien vaatimusten, kustannusten ja tietoturvallisuuteen kohdistuvan jäännösriskin[120] välillä.[121]

---

[116] VM 2022:43, s. 38
[117] HE 284/2018 vp, s. 92
[118] VAHTI 22/2017, s. 18
[119] VM 2022:43, s. 37–38
[120] VM 2021:65, s. 32 – jäännösriskillä tarkoitetaan niitä riskejä, jotka jäävät voimaan riskienhallintatoimenpiteiden jälkeen, eikä niihin voida tai haluta vaikuttaa.
[121] VM 2021:65, s.30

Tiedon elinkaari kattaa kokonaisuudessaan kaikki tiedon käsittelyn vaiheet, alkaen tiedon tuottamisesta tai vastaanotosta, säilytyksestä, käytöstä, jakamisesta, siirrosta ja loppuen tiedon arkistointiin tai tuhoamiseen. Tiedon elinkaariajattelun lähtökohtana osana tiedonhallintayksikön toimintaa pidetään tiedon suunnitelmallista ja riskilähtöistä käsittelyä ja hallintaa. Tietojärjestelmän elinkaari kattaa tiedon elinkaaren tavoin kaikki sen syntymisestä ja päättymisestä koskevat vaiheet alkaen tietojärjestelmän määrittelystä ja suunnittelusta, kilpailutuksesta ja hankinnasta, toteutuksesta ja kehityksestä, käyttöönotosta, ylläpidosta sekä päättyen käytöstä poistoon. Tietojärjestelmien elinkaariajattelun lähtökohtana on jokaisessa tietojärjestelmässä käsiteltävien tietojen elinkaaren huomiointi ja järjestelmien suunnitelmallinen ja riskilähtöinen hallinta osana tiedonhallintayksikön toimintaa. Tietoturvallisuus tietojärjestelmien ja tietoaineistojen elinkaaressa luo kokonaisuuden, johon sisältyvät riskien arviointi, tiedon luokittelu, tietoturvallisuustoimenpiteiden suunnittelu tunnettujen riskien pohjalta sekä tietoturvallisuustoimenpiteiden toteuttaminen.[122]

Tiedonhallintalain 13 §:n 1 momentti muodostaa kokonaisuuden, sisältäen riskien arvioinnin, tietoturvallisuustoimenpiteiden suunnittelun tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttamisen.[123]

13 §:n 2 momentissa säädetään viranomaisen olennaisten tietojärjestelmien vikasietoisuudesta ja toiminnallisesta käytettävyydestä varmistamisesta riittävän säännöllisellä testauksella. Säädös koskee tietojärjestelmien tietoturvallisuuden toteuttamiseen liittyvistä erityisvaatimuksista. Olennaisella tietojärjestelmällä tarkoitetaan niitä tietojärjestelmiä, jotka ovat kriittisiä viranomaisen lakisääteisten tehtävien toteuttamisen kannalta erityisesti silloin, kun tuotetaan palveluja hallinnon

[122] VM 2021: 65. s. 22
[123] HE 284/2018 vp, s. 92

asiakkaille[124]. Säännös ei näin ollen velvoita niitä viranomaisen tietojärjestelmiä, jotka eivät täytä olennaisen tietojärjestelmän määritelmää.

Tiedonhallintayksikön tulee tunnistaa olennaiset tietojärjestelmät osana riskienhallintaa.[125] Toiminnallisella käytettävyydellä tarkoitetaan, että tietojärjestelmä on helposti opittava ja sen toimintalogiikka on helposti muistettava sekä sen toiminta tukee niitä työtehtäviä, joita käyttäjän tulee tehdä edistäen käytön virheettömyyttä. Lainsäätäjä näkee tietojärjestelmien toiminnallisen käytettävyyden osana tietoturvallisuustoimenpiteitä, sillä mikäli tietojärjestelmä on vaikeasti opittava sekä toimintalogiikaltaan vaikea, voivat ne johtaa virheelliseen tietojärjestelmän käyttöön vaarantaen tietoturvallisuuden. Tietojärjestelmien toiminnallinen käytettävyys luo viranomaistoiminnasta tehokkaampaa, edistäen perustuslain 21 §:ssä säädettyä viranomaisen toiminnan viivytyksettömyysvaatimuksen toteutumista.[126]

Käytännössä tietojärjestelmien vikasietoisuus voidaan varmistaa erinäisillä tavoilla, kuten testauksella ennen tietojärjestelmän käyttöönottoa sekä merkittävien ylläpitotoimien yhteydessä, kuormitustestauksella sekä vikatilanteesta toipumisen suunnittelulla. Testauksien yhteydessä on laadittava raportteja siitä, mitä on testattu sekä millaisia tuloksia niissä on saatu. Raportit tulee myös huomioida osana järjestelmäkehitystä.[127]

13 §:n 3 momentissa edistetään hyvän julkisuus- ja salassapitorakenteen toteutumista osana viranomaisten tietojärjestelmiä sekä niissä olevissa tietoaineistoista muodostuvissa tietokannoissa. Säännöksellä pyritään varmistamaan tietojen saatavuus julkisuusperiaatteen toteuttamiseksi, viranomaisten tehtävien hoitamiseksi sekä salassapitointressin turvaamiseksi.[128]

---

[124] HE 284/2018 vp, s. 92-93.
[125] Voutilainen, 2019. s. 333
[126] HE 284/2018 vp, s. 92–93
[127] VM 2022:43. s. 35
[128] HE 284/2018 vp, s. 93

13 §:n 4 momentissa säädetään viranomaisen velvollisuudesta varmistaa osana hankintojaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. Tietojärjestelmien on täytettävä siinä käsiteltävien tietoaineistojen tietoturvallisuusvaatimukset sekä oltava käyttökelpoinen viranomaisen tehtävien hoitamiseksi tuloksekkaasti ja tehokkaasti [129] . Laissa ei ole säädetty tyhjentävästi tietojärjestelmien tai tietoaineistojen konkreettisista toimenpiteistä, vaan ne tulee määritellä ja toteuttaa tapauskohtaisesti kussakin tietojärjestelmässä niissä käsiteltävien tietojen laadun ja luonteen perspektiivistä [130] . Tietoturvallisuusriskien arvioinnin tuloksia voidaan hyödyntää soveltuvin osin hankintamenettelyssä[131]. Osana tietojärjestelmän tietoturvallisuustoimenpiteiden määrittelyä ja toteuttamista on otettava huomioon myös hankittavan tietojärjestelmän vaikutus viranomaisten tehtävien hoidolle, lakisääteisten velvollisuuksien toteuttamiselle ja yhteiskunnan toiminnalle[132].

Tiedonhallintalain 14 §:ssä säädetään viranomaisen salassa pidettävien tietojen siirtämisen perusteista tietoverkossa. Viranomaisen tulee toteuttaa tietojensiirto yleisessä tietoverkossa suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, mikäli siirrettävät tiedot ovat salassa pidettäviä. Säännös ei määrittele minkälaista yhteyttä tai tiedonsiirtotapaa viranomaisen tulisi käyttää, vaan toteutustapa jätetään viranomaisen omaan harkintaan. [133] Viranomaisen käytettävän salausratkaisun tulee kuitenkin perustua salassa pidettävän tiedon luokitteluun ja riskiarvioon [134] . Säädöksessä mainitulla yleisellä tietoverkolla tarkoitetaan internetiä, jolloin tiedonhallintalain 14 §:ää ei sovelleta niissä tilanteissa, kun tietojen siirtäminen tapahtuu muussa kuin yleisessä tietoverkossa, kuten viranomaisen sisäisessä verkossa[135].

---

[129] HE 284/2018 vp, s. 93
[130] VM 2021:65, s. 40
[131] Katakri, 2020, s. 11
[132] VM 2021:65, s. 40
[133] HE 284/2018 vp, s. 93
[134] VM 2021:65, s. 51
[135] HaVM 38/2018 vp, s. 24

Viranomaisen sähköpostin käyttöä salassa pidettävien tietojen sähköisenä tiedonsiirtomenetelmänä ilman asianmukaisia tiedon salaustoimenpiteitä on saanut laillisuusvalvonnassa useasti huomautuksia. Viranomaisen tulee salata viestinsä sisältö, vaikka siinä ilmenevät salassa pidettävät tiedot ovat saapuneet viranomaiselle asiakkaan toimesta avoimessa verkossa.[136] 14 §:n toisen virkkeen mukaan tiedonsiirto on järjestettävä niin, että ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja, on vastaanottaja tunnistettava riittävän tietoturvallisella tavalla. Säädöstä sovelletaan tunnistamisen tai varmistamisen osalta lähinnä viranomaisten välisessä viestinnässä, sillä yleisölle tarjottavien digitaalisten palveluiden tunnistamisen osalta sovelletaan lakia digitaalisten palvelujen tarjoamisessa (306/2019) säädettyä 6 §:ää[137].

Tiedonhallintalain 15 §:ssä säädetään tietoturvallisuuden varmistamisesta viranomaisen toiminnassa. Pykälän mukaan viranomaisen on varmistettava tietoturvallisuustoimenpiteiden avulla, että sen:

> *”1) tietoaineistojen muuttumattomuus on riittävästi varmistettu;*
> *2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;*
> *3) tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu;*
> *4) tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu;*
> *5) tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu;*
> *6) tietoaineistot voidaan tarvittavilta osin arkistoida.”*

15 §:n luomat velvollisuudet kohdistuvat viranomaisiin julkisuuslaista pohjautuvan erillisyysperiaatteen kautta, jonka mukaisesti viranomainen vastaa sen hallussa olevista asiakirjoista ja näin ollen myös tietoaineistoista. Säännöksen varmistamisvelvollisuudet koskevat viranomaisen kaikkia tietoaineistoja, riippumatta ovatko tietoaineistot tietojärjestelmissä, fyysisiä tai muulla tavalla tallennettuja.[138]

---

[136] Ks. OKV/1913/1/2018, OKV/1964/1/2017, OKV/96/1/2016, OKV/1131/1/2013, EOA/3438/4/2009
[137] HE 284/2018 vp, s. 94
[138] Voutilainen 2019, s. 335

15 §:n 1 momentin 1 kohdan mukaan tietoaineistojen muuttumattomuus on suojattava siltä osin, kun ne ovat tarpeellista pitää muuttumattomana. Tietoaineistojen muuttumattomuudella on etenkin niiden todistusvoimaisuuden kannalta tärkeässä roolissa. Tietoaineiston muuttumattomuuden varmistaminen vaihtelee tietoaineistojen välillä, mutta niiden muuttumattomuus tulisi varmistaa etenkin niissä tietoaineistoissa, joissa määritellään yksilöiden ja yhteisöjen etuja, oikeuksia ja velvollisuuksia. Tällöin voidaan varmistua asiakirjojen ja muiden tietojen aitoudesta ja alkuperäisyydestä sekä havaita mikäli niihin on tehty muutoksia. Säännöksessä ei määritellä sitä, miten muuttumattomuus varmistetaan, vaan luo viranomaiselle harkintamahdollisuuden riittävän muuttumattomuuden saavuttamiseksi. [139] Muuttumattomuuden varmistaminen on keskeinen osa tiedon eheyden turvaamista.

15 §:n 1 momentin 2 kohdan mukaan tietoaineistot tulee suojata teknisiltä ja fyysisiltä vahingoilta. Tietoturvallisuutta vaarantavia teknisiä vahinkoja ovat esimerkiksi kovalevyjen rikkoutuminen, jolloin ilman asianmukaisia varmuuskopioita voidaan tietoaineistot osin menettää pysyvästi. Fyysisiin vahinkoihin lukeutuu esimerkiksi konehuoneen tuhoutuminen sähkövian aiheuttaman tulipalon takia.

15 §:n 1 momentin 3 kohdassa säädetään tietoaineistojen alkuperäisyyden, ajantasaisuuden ja virheettömyyden varmistamisesta. Vaatimus on keskeisessä asemassa viranomasitoiminnan asianmukaisuuden takaamiseksi sekä hallinnon henkilökunnan sekä asiakkaiden oikeusturvan toteuttamiseksi ja takaamiseksi [140] . Tietoaineiston alkuperäisyys on yhteydessä tietojen muuttumattomuuteen ja todistusvoimaisuuteen. Käytännössä alkuperäisyydestä voidaan varmistua pitämällä huolta tiedon muuttumattomuuden vaatimuksesta. Viranomaisten on huolehdittava tietoaineistojen ajantasaisuudesta etenkin silloin, jos ne määrittelevät yksilön ja yhteisön etuja, oikeuksia ja velvollisuuksia. Ajantasaisuuden vaatimusta ei kohdisteta esimerkiksi

[139] HE 284/2018, s. 94
[140] HE 284/2018, s. 95

arkistoissa oleviin tiedostoihin. Tietoaineistojen virheettömyydellä on keskeisessä yhteydessä perustuslain 21 §:ssä säädettyyn oikeusturvaan ja hyvään hallintoon. Viranomaisen asiankäsittelyn tulee olla lähtökohtaisesti virheetöntä ja viranomaisten päätökset tulee pohjautua ajantasaiseen ja virheettömiin tietoihin. Ajantasaisuus ja virheettömyys turvaavat käsittelyn asianmukaisuutta ja oikeutta saada viranomaiselta asiasisällöltään virheetön sekä perusteltu päätös kohtuullisessa ajassa. [141] Laillisuusvalvoja on ratkaisussaan pitänyt itsestään selvänä lähtökohtana, että viranomaisten laatimat asiakirjat ja tiedostot ovat oikeita, virheettömiä ja ajantasaisia.[142]

15 §:n 1 momentin 4 kohdan viranomaisen tietoaineistojen saatavuuden ja käyttökelpoisuuden varmistamisen vaatimus on osa edellä esitetyn tietojen käytettävyyden varmistamista. Tietojen saatavuudella ja käytettävyydellä on viranomaisen toiminnan kannalta keskeinen asema nykyisessä tietointensiivisessä hallinnosta. Viranomainen on riippuvainen tietojen saatavuudesta käyttökelpoisessa muodossa varmistaakseen asianmukaisen viranomaistoiminnan. [143] Saatavuuden vaatimuksella on vahva yhteys julkisuuslain 1 §:n julkisuusperiaatteeseen, jonka mukaan viranomaisen asiakirjat ovat julkisia. Julkisuuslain nojalla viranomaisella on viivytyksettömyysvaatimus julkisia asiakirjoja annettaessa[144]. Tiedonhallintalain 1 §:n yhtenä tarkoituksena säädetäänkin tietoaineistojen tietoturvallisen käsittelyn varmistamisesta julkisuusperiaatteen toteuttamiseksi.

15 §:n 1 momentin 5 kohdan saatavuuden rajoittamisen vaatimus on kytköksissä myös viranomaisen julkisuusperiaatteeseen. Tiedon saatavuutta voidaan käytännössä rajoittaa niihin tietoaineistoihin, jotka sisältävät henkilötietoja tai erityisesti salassa pidettäviä tietoja. Saatavuuden rajoitukset eivät koske julkisia tietoaineistoja.[145]

---

[141] Voutilainen, 2019, s. 336
[142] AOKS OKV/1242/1/2013 28.4.2014
[143] HE 284/2018 vp, s.95
[144] Voutilainen, 2019, s.337
[145] HE 284/2018 vp, s. 95

15 §:n 1 momentin 6 kohdan vaatimus tietojen arkistoinnista tarpeellisin osin liittyy arkistolain luomien arkistointivelvollisuuksien varmistamiseen. Viranomaisen on varmistettava tietoaineistojen arkistointikelpoisuus. Arkistointikelpoisuudella tarkoitetaan tietoaineistojen tallennusmenetelmien toteuttamista niin, että niiden alkuperäisyys ja todistusvoimaisuus on mahdollista todentaa myös arkistossa.[146]

Tiedonhallintalain 16 §:ssä säädetään tietojärjestelmien käyttöoikeuksien hallinnan perusteista. Tiedonhallintamalleissa tulee määritellä tietojärjestelmien ylläpitoon liittyvät vastuut, sekä ilmetä kenelle vastuu käyttöoikeuksien määrittelystä, ylläpidosta ja ajantasaisuudesta kuuluu[147]. Käyttöoikeuksien hallinnassa tulee noudattaa vähempien oikeuksien periaatetta koko tietojärjestelmän elinkaaren ajalta. Vähempien oikeuksien periaatteella tarkoitetaan, että tietojärjestelmän käyttäjälle myönnetään vain sen laajuiset käyttöoikeudet, kun työtehtävän kannalta on tarpeellista[148]. Käyttöoikeuksien hallinnalla pyritään varmistumaan, että vain oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään tietoon, jota pyritään suojelemaan. Käyttöoikeudet tulee myöntää vain niille henkilöille, joiden käyttötarpeesta on varmistuttu.[149] Voutilainen näkee tiedonhallintalain 16 §:ssä säädetyn tietojärjestelmien käyttöoikeuksien säätelyn liittyvän osaksi hyvän julkisuus- ja salassapitorakenteen toteuttamista[150].

Tiedonhallintalain 17 §:ssä säädetään lokitietojen keräämiseen liittyvästä sääntelystä. Säädös edellyttää lokitietojen keräämistä vain silloin, kun tietojärjestelmän käyttö edellyttää tunnistautumista. Lokitietoja ei siis tarvitse kerätä yleisestä tietoverkosta, kuten verkkosivuilta. Lokitiedot on kerättävä tietojärjestelmän käytöstä ja tietojen luovutuksista. Tietojen luovuttamisesta kerättävien lokitietojen avulla voidaan varmistua tietojen luovuttamisen lainmukaisesta perusteesta.[151] Tietojärjestelmien lokitietojen

[146] Voutilainen, 2019, s. 338
[147] HE 284/2018 vp, s. 95
[148] VM 2021:65, s. 67
[149] VM 2022:43, s. 87
[150] Voutilainen, 2019, s. 333–334
[151] HE 284/2018 vp, s. 96

kerääminen on sidottu osaksi tietojen tarpeellisuutta, jota arvioidaan riskiperusteisesti. Käyttölokitietojen keräämisen tarpeellisuutta voidaan arvioida jakamalla niiden tarpeellisuus sen perusteella, tarvitaanko niitä osana virheselvittelyä, yksilön oikeuksien sekä oikeusturvan takaamiseksi vai virkavastuun todentamiseksi.[152]

Tiedonhallintalain 18 §:ssä säädetään turvallisuusluokiteltavista asiakirjoista valtionhallinnossa. Turvallisuusluokittelumerkintä on tehtävä valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien. Merkinnällä osoitetaan, minkälaisia tietoturvallisuustoimenpiteitä eri turvallisuusluokiteltua asiakirjaa käsitellessä noudatetaan.

Turvallisuusluokittelusta [153] säädetään tarkemmin valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Turvallisuusluokiteltavat asiakirjat jaetaan asetuksen 3 §:n mukaisesti neljään turvallisuusluokkaan salassa pidetyn tiedon oikeudettoman paljastuksen tai oikeudettoman käytön aiheuttaman suojattavan etuun kohdistuvan mahdollisen vahingon suuruuden mukaan. Korkein hallinto-oikeus on asiantuntijalausunnossaan koskien tiedonhallintalain esitystä huomauttanut luokittelusäännöksien perusongelmasta, jolloin tulkinnanvaraisessa tilanteessa asiakirja mahdollisesti merkitään varmuuden vuoksi luokitelluksi, johtaen julkisuuden kapenemiseen.[154]

Asiakirjan turvallisuusluokka	**Merkintä**	**Suojattavan edun vahinkojen suuruus**
1. turvallisuusluokka	ERITTÄIN SALAINEN (TL I)	Erityisen suuri
2. turvallisuusluokka	SALAINEN (TL II)	Merkittävän suuri

[152] VM 2021:65, s. 72
[153] Ks. VM 2021:5 – Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä
[154] KHO, 2019, s. 6

3. turvallisuusluokka	LUOTTAMUKSELLINEN (TL III)	Aiheuttaa vahinkoa
4. turvallisuusluokka	KÄYTTÖ RAJOITETTU (TL IV)	Lievä vahinko

3.1 Tiedonhallintoyksikkö viranomaisen tietoturvallisuuden järjestäjänä

Tietoturvallisuuden järjestämisen vastuu julkisessa toiminnassa on tiedonhallintayksiköllä. Tiedonhallintalaissa tiedonhallintayksiköllä tarkoitetaan sitä viranomaista, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti (TiHL 2 § 2 mom.). Tiedonhallintalain mukaiset tiedonhallintayksiköt ovat valtion virastot ja laitokset, tuomioistuimet ja valitusasioita käsittelemään perustetut lautakunnat, eduskunnan virastot, valtion liikelaitokset, hyvinvointialueet, hyvinvointiyhtymät, kunnat, kuntayhtymät, itsenäiset julkisoikeudelliset laitokset sekä yliopistolain mukaiset yliopistot sekä ammattikorkeakoululain mukaiset ammattikorkeakoulut (TiHL 4 § 1 mom.).

Tiedonhallintalaissa tiedonhallintayksikön johdolla tarkoitetaan sitä viranomaista tai virkamiestä, jonka vastuulla tiedonhallintayksikön, kuten valtion viraston tai kunnan yleisjohto kuuluu [155] . Tiedonhallintalaissa tiedonhallinnan järjestämisen vastuu on osoitettu tiedonhallintayksikön johdolle, jonka on huolehdittava tiedonhallinnan järjestämiseen liittyvien osa-alueiden vastuiden määrittelystä. Tiedonhallintayksikön johdon on myös valvottava aktiivisesti tiedonhallintaan liittyvien velvollisuuksien toteuttamista.[156]

Tiedonhallintalain 4 §:n 2 momentin luettelon 1 kohdan mukaisesti tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on määritelty tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut. Säännöksellä tarkoitetaan konkreettisten vastuiden määrittämistä siitä, miten ja kenen vastuulla lain

[155] VM 2020:18, s. 9
[156] VM 2020:18, s. 10

mukaisen velvoitteet ja palvelut toteutetaan. Vastuut tulee määritellä tiedonhallintamallin ylläpidon ja tietoaineistojen muodostamisen toteuttamiselle, tietoturvallisuuden ja asianhallinnan järjestämiselle, tietojärjestelmien yhteen toimivuuden turvaamiselle sekä tietoaineistojen säilyttämisen järjestämiselle. [157] Tiedonhallintalain 4 §:n 2 momentin luettelon 2 kohdan mukaisesti johdon tulee huolehtia ohjeiden ajantasaisuudesta. Tiedonhallintayksiköllä tulee olla ohjeet siitä, miten tietoaineistoja käsitellään osana toimintaprosessia. Tietojärjestelmien käytöstä tulee olla ajantasaiset ohjeet niin, että tietojärjestelmien käyttäjät tietävät ja saavat selon siitä, miten tietojärjestelmiä käsitellään tietoturvallisella tavalla lainmukaisiin käyttötarkoituksiin.[158] Tiedonhallintalain 4 §:n 2 momentin luettelon 3 kohta edellyttää tiedonhallintayksikköä huolehtimaan tarpeellisesta koulutuksesta liittyen tiedonhallinnan menettelytapojen, sovellettavan lainsäädännön, asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä sekä tiedonhallintayksikön tai siinä toimivien viranomaisten määräyksistä sekä ohjeista tiedonhallinnan toteuttamiseksi [159] . Tiedonhallintalain 4 §:n 2 momentin luettelon 4 kohdan perusteella johdon vastuulla on huolehtia asianmukaisista työvälineistä viranomaisen tiedonhallintaa koskevien velvollisuuksien täyttämiseksi niin, että viranomaiset voivat hoitaa tiedonhallintaan liittyvät tehtävänsä hyvän hallinnon edellyttämällä tavalla tehokkaasti ja tuloksellisesti. Säännöksellä korostetaan sitä, että työvälineet ovat ajantasaisia ja riittävän suojattuja siten, että niiden käyttö tukee viranomaisen tehtävien hoitamista hyvän hallinnon edellyttämällä tavalla. Työvälineiden asianmukaisuuden varmistamiseen kuuluu myös hankintojen sekä laitesopimuksien asianmukaisuuden varmistaminen [160] . Johdon vastuulla on myös tiedonhallintalain 4 §:n 2 momentin luettelon 5 kohdan mukaisesti riittävän valvonnan järjestäminen tiedonhallinnan säädösten, määräysten ja ohjeiden noudattamiseksi. Johdon tulee siis huolehtia siitä, että tiedonhallintayksikössä on olemassa riittävät kontrollit, joiden avulla varmistetaan, että tiedonhallintayksikössä toimivat viranomaiset noudattavat tiedonhallintaa koskevia laissa säädettyjä

[157] HE 284/2018, s. 73
[158] HE 284/2018, s. 73
[159] HE 284/2018, s. 74
[160] VM 2020:18, s. 16

vaatimuksia ja että tiedonhallintayksikön sisäisiä määräyksiä ja ohjeita liittyen tiedonhallintaan noudatetaan. Valvonnan järjestäminen käsitetään osaksi tiedonhallintayksikön sisäisen valvonnan järjestelyjä ja tietoturvallisuustoimenpiteiden toteuttamista.[161]

3.2 Tiedonhallintalautakunta

Tiedonhallintalain tullessa voimaan osana lakia säädettiin julkisen hallinnon tiedonhallintalautakunnasta, joka toimii itsenäisenä viranomaisena valtiovarainministeriön yhteydessä. Tiedonhallintolautakunnan tehtävät liittyvän nimenomaisesti tiedonhallintalaista kumpuavien tiedonhallintaa ja tietoturvallisuutta edistävien menettelytapojen sekä vaatimuksien toteuttamiseen. Osana tätä tehtävää tiedonhallintalautakunta julkaisee valtiovarainministeriön yhteisötekijänä suosituksia tiedonhallintalain soveltamisesta, joita myös tässä tutkielmassa on hyödynnetty laajasti.

Tiedonhallintalautakunnan toimivalta rajataan tiedonhallintalain 3.3 §:ssä koskemaan hyvinvointialueita, hyvinvointiyhtymiä, kuntia ja kuntayhtymiä niiden hoitaessa laissa säädettyjä tehtäviä. Tiedonhallintalautakunnan ohjaus- ja valvontatehtäviin ei kuulu eduskunnan oikeusasiamiehen, valtioneuvoston oikeuskanslerin, tuomioistuimien, valitusasioita käsittelemään perustetut lautakunnat, tasavallan presidentin kanslia, eduskunnan virastot, Kansaneläkelaitos, Suomen Pankki, itsenäiset julkisoikeudelliset laitokset, yliopistolain mukaiset yliopistot sekä ammattikorkeakoululain mukaiset ammattikorkeakoulut.

Tiedonhallintalain 10 §:ssä säädetään tiedonhallintalautakunnan tehtävistä.

> *”1) arvioida valtion virastojen ja laitosten, hyvinvointialueiden ja hyvinvointiyhtymien sekä kuntien ja kuntayhtymien 4 §:n 2 momentin, 5, 19, 22–24, 24 a, 24 b ja 28 §:n sekä 6 luvun säännösten toteuttamista ja noudattamista;*

[161] HE 284/2018, s. 74

2) edistää tässä laissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tämän lain vaatimusten toteuttamista." (TiHL 10 § 1 ja 2 mom.)

Tiedonhallintalautakunnan arviointitehtävästä säädetään tarkemmin tiedonhallintalain 11 §:ssä seuraavasti:

"Tiedonhallintalautakunnan arviointitehtävän toteuttaminen perustuu tiedonhallintalautakunnan hyväksymään arviointisuunnitelmaan." (TiHL 11 § 1 mom.)

Lisäksi tiedonhallintalain 11 §:n 2 momentissa säädetään tiedonhallintalautakunnan oikeuksista saada arviointitehtävän toteuttamiseksi arvioinnin kohteena olevilta viranomaisilta salassapitosäännösten estämättä arviointitehtävän hoitamiseksi välttämättömät selvityksen ja tarpeelliset tiedon maksutta. Viranomaisen tulee toimittaa pyydetyt tiedot asetettuun määräaikaan mennessä tiedonhallintalautakunnalle. Tiedonhallintalain 11 §:n 4 momentissa säädetään myös tiedonhallintalautakunnan velvollisuudesta laatia kertomus joka toinen vuosi arvioinnin tuloksista joka on toimitettava valtiovarainministeriölle. Toistaiseksi tiedonhallintalautakunta on toteuttanut yhden arviointikertomuksen vuonna 2021, jolloin arviointikohteet olivat asiakirjajulkisuuskuvaukset, tiedonhallintamalli, muutosvaikutusten arviointi sekä tiedonhallintalain 22 §:n 3 momentin mukaiset tietojärjestelmien teknisten rajapintojen määrittelyt ja ylläpito[162].

Tiedonhallintalautakunnan tehtävä ei siis ole niinkään laillisuusvalvonnan toteuttaminen, vaan se keskittyy arvioimaan ja edistämään viranomaisen tiedonhallintalaista kumpuavien vaatimuksien toteutumista tiedonhallinnan ja tietoturvallisuuden osalta. Tietosuojavaltuutettu valvoo tiedonhallintalain tietoturvatoimenpiteitä, jotka koskevat tietosuojalainsäädännön mukaisia teknisiä ja organisatorisia toimia henkilötietojen suojaamiseksi, kun taas muut tietoturvajärjestelyt ovat osa yleistä laillisuusvalvontaa[163].

[162] VM 2022:8, s. 10
[163] Voutilainen, 2023, s. 422

4 Hyvän hallinnon monet ulottuvuudet

Hyvän hallinnon käsitettä ei mainittu suomalaisessa lainsäädännössä varsinaisesti ennen vuotta 1995, jolloin hyvän hallinnon vaatimuksien perusoikeudellinen asema vahvistettiin osaksi suomen kansallista lainsäädäntöä[164]. Hyvän hallinnon periaatteet vakiintuivat kansallisen hallinto-oikeuden periaatteiksi vuonna 2003 osana uutta hallintolakia. Hyvän hallinnon käsite vakiintui kuitenkin huomattavasti aikaisemmin osaksi oikeusjärjestelmäämme, ensi sijassa oikeuskanslerin ja eduskunnan oikeusasiamiehen ratkaisujen pohjalta 1970-luvulla[165].

Hyvää hallintoa on käsitelty suomalaisessa oikeuskirjallisuudessa erittäin kattavasti, missä sen sisältö on saanut useita erinäisiä määritelmiä sekä näkökulmia. Etenkin vuonna 2003 säädetyn hallintolain jälkeen on sen esiintyminen hallinto-oikeudellisessa kirjallisuudessa kasvanutkin merkittävästi, jonka jälkeen hyvän hallinnon käsitykset oikeuskirjallisuudessa ovat jaettavissa lähtökohtaisesti suppeisiin ja laajoihin käsitystapoihin[166].

Suppean käsitystavan mukaisesti hyvä hallinto nähdään pitävän sisällä perustuslain 21 §:än, virkavastuun toteuttamisen mahdollisuuden sekä oikeudet tulla kuulluksi, saada perusteltu päätös ja oikeuden muutoksenhakuun[167]. Perustuslain 21 §:n mukaisesti:

> *”Jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi.*
>
> *Käsittelyn julkisuus sekä oikeus tulla kuulluksi, saada perusteltu päätös ja hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet turvataan lailla.”*

---

[164] Laki suomen hallitusmuodon muuttamisesta (969/1995).
[165] Heuru, 2003, s. 141
[166] Heuru, 2003, s. 146
[167] Heuru, 2003, s. 146

Hahmottaessa hyvän hallinnon käsitettä sen suppeasta näkökulmasta, on hyvälle hallinnolle hahmotettavissa jossain määrin rajat kansallisessa lainsäädännössä.

Laaja käsitystapa omaksuu säädetyn lain ulkopuolelta tulevat vaikutteet osaksi hyvän hallinnon käsitteistöä. Laajassa käsitystavassaan hyvä hallinto nähdään tietynlaisena hallinnollisen kulttuurin kehitysilmiönä, josta on johdettavissa jopa oikeus- ja moraaliperiaatteiden tasoisia näkökulmia. [168] Laajassa käsitystavassaan hyvälle hallinnolle on ominaista sen muuttuminen jatkuvasti vallitsevan oikeuskulttuurin mukaisesti, pitäen sisällään eräänlaisia sukupolvenomaisia kerroksia tai yleisesti hyväksyttyjä tapoja. Vallitseva ajan henki ja hallintoideologia vaikuttavat jopa huomaamattaan hyvän hallinnon käsitteeseen, luoden uusia ilmentymiä sekä muunnelmia hyvän hallinnon käsitteeseen.[169]

Hyvän hallinnon yhteydessä mainitaan usein siihen yhdistettävä hyvän hallintotavan vaatimus. Käsitteen sisällöstä on varsin ristiriitaisia tulkintoja, eikä hyvän hallintotavan ja hyvän hallinnon käsitteellinen suhde ole erityisen vakiintunut [170]. Hyvä hallintotapa yleisesti voidaan nähdä oikeudellisessa argumentaatiossa käytettävänä yleiskäsiteenä, joka toimii hyvän hallinnon säädännöllisen sisällön laajennuksena ja uuden sisällön luomisessa hallintomenettelyihin liittyvien tulkintaratkaisujen tukemiseksi [171]. Usein hyvän hallinnon ja hyvän hallintotavat käsitteet nähdäänkin synonyymeinä suhteessa toisiinsa. Se voidaan kuitenkin hahmottaa olevan hallinto-oikeuden sääntelyn päämäärä, sekä sitä voidaan kuvailla tietynlaisena sateenvarjona, joka peittää alleen kokoelman erinäisiä sääntöjä ja periaatteita.[172]

Hyvän hallinnon sisältö on varsin epämääräinen ja vaikeasti kuvattavissa tyhjentävästi etenkin sen laajassa käsitystavassaan, jolloin sen sisältö jää jossain määrin avoimeksi.

---

[168] Heuru, 2003, s. 146
[169] Koivisto & Koulu, s. 809-810
[170] Koivisto, 2011, s. 122
[171] Voutilainen, 2007, s. 24
[172] Koivisto, 2011, s. 5

Tosin hyvän hallinnon käsitteellisen sisällön määrittäminen tyhjentävästi ei välttämättä olekaan tarkoituksenmukaista, sillä sitä kuvaa eräänlainen jatkuva muutos hyvyyden sisällöstä. Se mitä käsitettiin viime vuosituhannella hyväksi hallinnoksi, on eittämättä muuttunut 2000-luvulla digitalisaation ja muiden hallintoon vaikuttaneiden muutosten myötä. Hyvän hallinnon sisällön tuleekin tällöin mukautua muutoksen mukana, jotta se vastaa tämän hetkistä tosiasiallista käsitystä hyvästä hallinnosta.

4.1 Hyvä hallinto perusoikeutena

Hyvän hallinnon perustusoikeudellinen asema ilmenee perustuslain 21 §:ssä, jossa määritellään sen lisäksi myös hallintomenettelyn perusteiden ja oikeusturvan perusoikeudet.

> *Jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi.*
>
> *Käsittelyn julkisuus sekä oikeus tulla kuulluksi, saada perusteltu päätös ja hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet turvataan lailla (PeL 21 §).*

Perustuslain 21 §:ssä esiintyvät menettelylliset perusoikeudet voidaan kokonaisuudessaan nähdä kuuluvan osaksi hyvän hallinnon takeita. Tällöin hyvä hallinto perusoikeutena pitää sisällään ainakin seitsemän pykälästä eriteltävää menettelyoikeutta:

1) oikeus saada asiansa käsitellyksi asianmukaisesti
2) oikeus saada asiansa käsitellyksi ilman aiheetonta viivytystä
3) oikeus saada asiansa käsitellyksi toimivaltaisessa viranomaisessa
4) hallintoasian käsittelyn julkisuus
5) oikeus tulla kuulluksi hallintoasiaa käsiteltäessä
6) oikeus saada perusteltu päätös hallintoasiassa ja

7) oikeus hakea muutosta hallintoasiassa annettuun päätökseen[173]

Perustuslain 21 §:n sisältämät menettelylliset oikeudet eivät määrittele hyvän hallinnon takeita kokonaisuudessaan, sillä 21 §:n 2 momentin mukaisesti myös muut hyvän hallinnon takeet tulee turvata lailla[174]. Tällaisia perustuslaissa säädettyjä muita hyvän hallinnon takeita ovat yhdenvertaisuuden vaatimus (PeL 6 §), kielelliset perusoikeudet (PeL 17 §), asiakirjajulkisuus (PeL 12 § 2 mom.), yksilön osallistumismahdollisuuksien edistäminen yhteiskunnalliseen toimintaan sekä häntä itseään (PeL 14 § 3 mom.) että elinympäristöönsä (PeL 20 § 2 mom.) koskevaan päätöksentekoon.[175]

Hyvän hallinnon perusoikeudellinen asema asettaa sille myös perusoikeuksiin liittyviä erityispiirteitä. Perustuslain 22 §:ssä säädetyn perusoikeuksien turvaamisvelvoitteen mukaisesti julkisen vallan on turvattava perus- ja ihmisoikeuksien toteutuminen. Viranomaisen on myös tällöin pyrittävä toiminnassaan aktiivisesti toteuttamaan hyvän hallinnon takeita[176]. Hyvän hallinnon takeilla on myös perusoikeusasemansa takia etusija suhteessa muuhun lainsäädäntöön. Jos tuomioistuimen käsiteltävänä olevassa asiassa lain säännöksen soveltaminen olisi ilmeisessä ristiriidassa perustuslain kanssa, tuomioistuimen on annettava etusija perustuslain säännökselle (PeL 106 §). Jos asetuksen tai muun lakia alemman asteisen säädöksen säännös on ristiriidassa perustuslain tai muun lain kanssa, sitä ei saa soveltaa tuomioistuimessa tai muussa viranomaisessa (PeL 107 §).

Valtiosääntökäytännössä on vakiintunut tapa tulkita hyvän hallinnon osatekijöitä perusoikeusmyönteisesti. Perusoikeusmyönteisyys tarkoittaa, että viranomaisen on valittava useista vaihtoehtoisista menettelytavoista tai tulkinnoista sellainen, joka edistää parhaiten asianmukaista menettelyä ja hyvää hallintoa[177].

[173] Mäenpää, 2023, s. 91
[174] Mäenpää, 2023, s.91
[175] Kulla & Salminen, 2021, s.41.
[176] Mäenpää, 2021, s. 4
[177] Mäenpää, 2021, s. 4

Perustuslain lisäksi hyvä hallinnon sisältöä käsitellään keskeisesti hallintolain 2 luvussa, jossa määritellään hyvän hallinnon perusteet. Hallintolain 2 luku koostuu hallinnon oikeusperiaatteista (6 §), palveluperiaatteen ja palvelun asianmukaisuudesta (7 §), neuvonnasta (8 §), hyvän kielenkäytön vaatimuksesta (9 §) ja viranomaisten yhteistyöstä (10 §). Hallintalain luetteloa ei ole tarkoitettu tyhjentäväksi, vaan osa hyvän hallinnon sisällöstä säädetään muissa lainsäädännöissä sekä osana oikeuskäytäntöä[178].
Lainsäätäjä on tavoitteissaan nähnyt hyvän hallinnon perusteet hallinnon toiminnan laadullisina vaatimuksina[179].

Hallintolain 6 §:ssä on säädetty hallinnon viidestä keskeisistä oikeusperiaatteesta:

1) yhdenvertaisuusperiaate
2) tarkoitussidonnaisuuden periaate
3) puolueettomuusperiaate
4) suhteellisuusperiaate
5) luottamuksensuojaperiaate

Yhdenvertaisuusperiaatteen mukaan viranomaisen ja virkamiehen on kohdeltava hallinnossa asioivia tasapuolisesti. Tarkoitussidonnaisuuden periaate velvoittaa viranomaista käyttämään toimivaltaansa yksinomaan laissa perusteltuihin tarkoituksiin. Puolueettomuusperiaatteen mukaisesti viranomaisen toimina on oltava puolueetonta sekä objektiivisesti perusteltavaa, sekä suhteellisuusperiaatteen mukaisesti oikeassa suhteessa laissa tavoiteltuun päämäärään nähden. Luottamuksensuojaperiaatteen mukaisesti viranomaisen toimien tulee suojata oikeusjärjestyksen takaamia oikeutettuja odotuksia. [180] Hallinnon oikeusperiaatteet ovat pääsääntöisesti aineellisia ratkaisuperiaatteita, sillä ne asettavat hallintotoiminnalle sisällöllisiä laatuvaatimuksia[181].

[178] Kulla & Salminen, 2021, s.109
[179] HE 72/2002, s 33
[180] Mäenpää, 2021, s. 89–90.
[181] Kulla & Salminen, 2021, s. 109–110

Osana hyvän hallinnon perusteita voidaan käsittää myös sellaisia periaatteita, joista säädetään hallintolain 2 luvun ulkopuolella koskien hallintoasian käsittelyä. Tällöin myös hallintolaissa säädetyt oikeusturvan, palvelujen laadun ja tuloksellisuuden edistäminen (HaL 1 §), käsittelyn viivytyksettömyys (HaL 23 §) ja esteellisyysperusteiden huomioon ottaminen (HaL 27-30 §) voidaan käsittää osaksi hyvän hallinnon perusteita. Myös perustuslain 21 §:ssä mainitut hyvän hallinnon takeiden vaatimuksia täydentävät oikeudet, oikeus asianmukaiseen käsittelyyn (PeL 21 § 1 mom.), oikeus toimivaltaiseen viranomaiseen (PeL 21 § 1 mom.), oikeus tulla kuulluksi (HaL 34§) sekä oikeus saada perusteltu päätös (HaL 45 §) käsitetään osaksi hyvän hallinnon perusteita.[182]

4.2 Sähköinen hallinto

Verkkoyhteiskunnan sekä digitalisaation kehittyessä on oikeus- ja hallintotieteelliseen keskustellun tullut mukaan sähköisen hallinnon käsite. Sähköistä hallintoa ei ole laintasolla määritelty, jolloin sen käsitteellinen sisältö ei ole kovinkaan tarkka. Sähköisen hallinnon käsitteestä onkin tutkimusyhteisössä esitetty hieman eriäviä näkemyksiä siitä.

Euroopan komissio on hahmottanut tiedonannossaan sähköisen hallinnon (eGovernment) näkökulmia ja sen mahdollisia muutoksia hallintoon. Sähköinen hallinto käsitetään tieto- ja viestintäteknologioiden käytöksi julkisessa hallinnossa yhdistettynä organisaatiomuutoksiin ja uusiin taitoihin, joiden avulla pyritään parantamaan julkisia palveluita ja demokraattisia prosesseja sekä julkisen politiikan legitimiteettiä. Sähköinen hallinto käsitetään paremman ja tehokkaamman hallinnon mahdollistajana, auttaen julkista sektoria selviytymään ristiriitaisista vaatimuksista tarjota enemmän ja parempia palveluita vähemmillä resursseilla. Sähköisellä hallinnolla tavoitellaan avointa ja läpinäkyvää hallintoa, joka on ymmärrettävä ja vastuullinen kansalaisille, mahdollistaen demokraattisen osallistumisen ja tarkastelun. [183]

[182] Mäenpää, 2023, s. 324
[183] COM (2003/567) final, s. 7-8

Voutilainen (2007) käsittää väitöskirjassaan sähköisen hallinnon toiminnallisena prosessikokonaisuutena, jossa hyödynnetään informaatio- ja viestintäteknologisia palveluita, joihin lainsäädännöllisten asinankäsittelyprosessien eri vaiheet ja niihin liittyvät viranomaistoiminnot tukeutuvat. Sähköinen hallinto koostuu näin kolmesta osasta: sähköisistä palveluista, sähköisestä asianhallinnasta ja perus- ja taustajärjestelmistä.[184].

Saarenpää (2004) on jäsentänyt yleisesti sähköisen hallinnon ja hyvän hallinnon yhteensovittamisen kannalta seitsemän keskeistä jännitettä. Nämä jännitteet liittyvät yksilön itsemääräämisoikeuden laajuuteen, hallinnon rooliin oikeusvaltiossa, automaattiseen päätöksentekoon, hallinnon avoimuuteen, tietokoneohjelmien avoimuuteen, yksityisyyteen, hallinnon yhteisiin tietovarantoihin ja asiakirjojen julkisuuteen sähköisessä hallinnossa. [185] Saarenpää (2023) on huomauttanut myöhemmin sähköisen hallinnon käsitteen suppeasta näkökulmasta käsittää tietotekniikan hyödyntäminen hallintotoiminnassa. Sähköisen hallinnon arviointi tapahtuu usein sähköisten asiointi- ja mobiilipalveluiden määrällä, jolloin sähköisyys nähdään enemminkin apuvälineenä hallinnon tehokkuutta edistäessä sivuuttaen kansalaisen oikeudet[186]. Saarenpää onkin nähnyt informaatiohallinnon osuvampana käsitteenä sähköisen hallinnon sijasta.[187]

Hahmottaessaan sähköisestä hallinnosta esiintyviä erityispiirteitä hyvän hallinnon takeiden toteutumiselle Voutilainen on esittänyt lisäksi sähköisen hyvän hallinnon käsitteen, johon kuuluvat sähköinen asianhallinta, tietoturvallisuus, viranomaisten julkisuus- ja salassapitorakenne, laadukkaat sähköiset asiointipalvelut sekä tehokkaat ohjelmistotuotantomenetelmät[188]. Sähköisen hyvän hallinnon normiperustan hän näkee kumpuavan perustuslain 21 §:stä, hallintolain hyvän hallinnon perusteista sekä

[184] Voutilainen, 2007, s.2-3.
[185] Saarenpää, 2004, s. 259-260
[186] PeVL 7/2019, s. 9: Perustuslakivaliokunta on myös maininnut hallintolain 1 §:n hyvän hallinnon perusteiden ja oikeusturvan ensisijaisuudesta suhteessa hallinnon tuloksellisuuteen.
[187] Saarenpää & Riekkinen, 2023, s. 77-78
[188] Voutilainen, 2009, s. 44

digipalvelulaista ja sähköisestä asioinnista annetuista säädöksistä. Sääntelykokonaisuudessa digipalvelulaki asettaa viranomaisten digitaalisten palveluiden järjestämistä edellyttävät velvollisuudet, missä sähköisestä asioinnista annettu laki säätää sähköisen hallinnon menettelysäännöksistä.[189]

Hyvän sähköisen hallinnon käsite heijastaa hyvän hallinnon monipuolisuutta ja historiallista kehitystä, joka antaa uusia merkityksiä käsitteelle hallinnon kehittyessä. Merkittävä ja jatkuvasti laajeneva osa hallinnon toiminnasta perustuu jo sähköisen hallinnon käyttämiin informaatio- ja viestintäteknologisiin ratkaisuihin, mikä tekee teknologian käytöstä olennaisen osan modernia hallintotoimintaa. Tällöin digitalisaation edistyessä hyvän sähköisen hallinnon käsite voi mahdollisesti saada entistä suuremman merkityksen erityisesti hallinnon tarjoamien digitaalisten palveluiden osalta, mikä ei välttämättä ole tarkoituksenmukaista hyvän hallinnon kannalta.

Tutkielman kannalta hallinnon sähköistyminen on keskeinen ilmiö, sillä juuri hallinnon sähköistymisen seurauksesta on noussut esiin uusia tarpeita säätää viranomaisen tietoturvallisuudesta. Seuraavassa kappaleessa paneudunkin tietoturvallisuuden ja hyvän hallinnon väliseen suhteeseen tarkemmin.

[189] Voutilainen, 2019, s. 194-195.

5 Hyvän hallinnon tietoturvallisuus

Voutilainen (2006) on hahmottanut tarkemmin tietoturvallisuuden lainsäädännöllistä suhdetta hyvän hallinnon säännöstöön kuuluviin erinäisiin elementteihin. Väitöskirjassaan hän hahmottaa tietoturvallisuuden sidonnaisuuden osaksi hyvän sähköisen hallinnon perustuslaillista säännöstöä ainakin PeL 21 §:n oikeuden saada asiansa käsitellyksi ilman aiheetonta viivytystä, PeL 10 §:n yksityiselämän kunnian ja kotirauhan sekä luottamuksellisen viestin salaisuuden, PeL 12 §:n julkisuuden ja PeL 7 §:n oikeuden henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen osalta[190].

Saarenpää (2023) hahmottaa lisäksi vaatimuksen julkisen vallan tietojärjestelmien laadukkaasta ja häiriöttömästä toiminnasta osaksi perustuslain 21 §:n takaamaa oikeusturvaa sekä hyvän hallinnon periaatteita. [191] Laadulla viranomaisen tietojenhallinnassa tarkoitetaan siitä huolehtimista, että tietoaineistojen ajantasaisuus, virheettömyys ja käyttökelpoisuus on varmistettu[192]. Oikeus laatuun käsitetään myös yhtenä verkkoyhteiskunnan metaoikeutena, jossa on pohjimmiltaan kysymys oikeuden ja erityisesti yksilön oikeuksien sekä oikeudellisesti suojattujen etujen vakavasti ottamisesta[193].

Tietojärjestelmien kuin myös tiedonhallinnan laadusta huolehtiminen ja toiminnan häiriöttömyydestä takaaminen ovat tietoturvallisuuden ydintä. Tietoturvallisuustoimenpiteet ovat niitä hallinnollisia toimenpiteitä, joilla varmistetaan tietoturvallisuuden ominaisuuksien laatu. Laillisuusvalvonnassa onkin korostettu, että tietojärjestelmistä kumpuavilla ongelmilla ei voida perustella hyvän hallinnon

[190] Voutilainen, 2007, s. 115–116
[191] Saarenpää & Riekkinen, 2023, s. 79
[192] HE 284/2018 vp, s. 60. Ajantasaisuus, virheettömyys ja käyttökelpoisuus kuuluvat tietoturvallisuuden ominaisuuksien (käytettävyys, eheys, luottamuksellisuus) käsitteistöön. Ks. 2. luku
[193] Pöysti, 2002, s. 71

säännöstöstä poikkeamista [194] . Viranomaisen tuleekin tällöin huolehtia tietoturvallisuustoimenpiteiden laadusta ja asianmukaisuudesta, jotta hyvän hallinnon asettamat vaatimukset toteutuvat. Tietoturvallisuuden merkityssisällön tarkempaa hahmottamista on syytä hakea muista hyvän hallinnon yksittäisistä tunnusmerkeistä.

5.1 Julkisuusperiaatteesta

Viranomaisen toimintaan vaikuttaa olennaisesti julkisuusperiaate. Julkisuusperiaate on hallinnon avoimuuden keskeinen osatekijä, jota on syytä pitää samalla yhtenä hyvän hallinnon keskeisenä edellytyksenä. Julkisuuden perusoikeudellinen asema ilmenee selkeästi perustuslaissa.

> *”Viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta.” (PeL 12 § 2 mom.)*

Lisäksi vaatimus käsittelyn julkisuudesta esiintyy myös perustuslaissa yhtenä hyvän hallinnon keskeisenä takeena.

> *”Käsittelyn julkisuus sekä oikeus tulla kuulluksi, saada perusteltu päätös ja hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet turvataan lailla.” (PeL 21 § 2 mom.)*

Viranomaisen tiedonhallintavelvoitteista säädetyssä tiedonhallintalaissa julkisuusperiaatteen ja tietoturvallisuuden välinen yhteys esiintyy keskeisessä osassa lain tarkoituksessa.

> *”varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi” (TiHL 1 § 1 mom.)*

---

[194] EOA 537/4/10, 12.8.2010

Lisäksi tiedonhallintalain neljännen kappaleen tietoturvallisuutta koskevilla säännöksillä on lain valmisteluaineistossa nähty olevan laillisen ja asianmukaisen tietojenkäsittelyn varmistamisesta koskevien toimenpiteiden niin tietosuojan, asiakirjajulkisuuden kuin hyvän hallinnon sekä oikeusturvan toteuttamiseksi[195].

Julkisuusperiaatteen neljä keskeistä toteuttamismuotoa ovat asiakirjajulkisuus, käsittelyn julkisuus, viranomaisten tiedottaminen sekä tiedonhallinta[196]. Viranomaisen julkisuuden toteuttaminen perustuu oletusarvoiseen julkisuuteen sekä sisäänrakennettuun julkisuuteen. Oletusarvoisella julkisuudella tarkoitetaan yleistä lähtökohtaa, jonka mukaan viranomaisen asiakirjat ovat julkisia. Sisäänrakennetulla julkisuudella tarkoitetaan viranomaisen toimia julkisuuden toteuttamiseksi, edellyttäen viranomaisen toiminnan järjestämistä julkisuusperiaatteen toteuttamiseksi niin, että tietoturvallisuuden vaatimukset otetaan huomioon.[197] Tietoturvallisuustoimenpiteet voidaan käsittää osaksi julkisuuden edellytysten ylläpitoon ja varmistamiseen[198].

5.1.1 Julkisuuden rajoitus ja salassapitovelvoitteet

Tietoturvallisuustoimenpiteiden suhde julkisuuteen etenkin salassapitovelvoitteiden osalta näyttäytyy merkittävänä, vaikka niiden suhde ei välttämättä ole niinkään suoraviivainen. Julkisuutta sääntelevät salassapitovelvoitteet ensisijaisesti rajoittavat tiedon saatavuutta, missä julkisuussäännöstö yleisesti puoltaa avoimuutta ja tietojen saatavuutta[199]. Salassapitovelvoitteiden tehtävänä on rajoittaa yleistä oikeutta saada asiakirja nähtäväksi tai siitä kopio niiltä osin kuin se on salassa pidettävä[200]. Julkisuutta ohjaa kuitenkin julkisuuslain 10 §:än tietynlainen julkisuuden maksimointivaatimus: jos vain osa asiakirjasta on määritetty salassa pidettäväksi, on silloin tieto annettava asiakirjan muusta osasta[201]. Turvallisuusluokitellut asiakirjat ovat aina myös salassa

[195] HE 284/2018 vp, s.149
[196] Mäenpää, 2020, s. 6
[197] Mäenpää, 2020, s. 17
[198] Mäenpää, 2018, s. 836
[199] Mäenpää, 2020, s. 283
[200] Wallin & Konstari, 2000, s. 134
[201] Wallin & Konstari, 2000, s. 121

pidettäviä, joten julkisuuslain 22 ja 23 §:n vaatimukset salassapidosta, vaitiolovelvollisuudesta ja hyväksikäyttökiellosta sekä tiedonhallintalain säännökset koskevat myös turvallisuusluokiteltua aineistoa[202].

Perustuslain 12.2 §:n mukaisesti julkisuudelle voidaan asettaa rajoituksia vain välttämättömistä syistä. Asiakirjan tai tiedon turvallisuusluokittelu tietoturvallisuussäännösten mukaan voivat käytännössä tarkoittaa sen julkisuuden rajoittamista joltain osin tai jossain suhteessa. Mikäli turvallisuusluokittelulla on julkisuutta rajoittava vaikutus, on rajoituksen perusteiden täytettävä julkisuuden yleiset edellytykset.[203] Julkisuuden rajoittamisen sisällölliset edellytykset koskevat ensisijaisesti rajoituksen välttämättömyyttä ja perusteltavuutta. Arvioitaessa tiedon rajoittamisen välttämättömyyttä, keskeinen merkitys on niiden oikeuksien ja etujen painavuudella joita rajoittamisella pyritään suojata. Tiedon julkisuuden rajoittamisen perusteltavuudella tarkoitetaan, että rajoittamiselle on asiallisesti hyväksyttävää syy. Julkisuuden rajoittamisen keskeisinä syinä ovat usein yleisen edun ja yksityisen intressin suojaaminen.[204]

5.2 Tietoturvallisuuden ominaisuudet osana julkisuuden toteuttamista

Tiedon saatavuus osana viranomaistoimintaa tarkoittaa asiakirjojen julkisuudesta ja salassapidosta huolehtimista sekä viranomaistoimintaa koskevien tietojen tuottamista ja jakelua. Viranomaisen tulee huolehtia myös siitä, että sen laissa säädettyjen tehtävien hoitoon tarvitsemat tiedot ovat saatavilla.[205] Tiedon saatavuuteen käsitettävällä tiedon käytettävyydellä tarkoitetaan julkisuuslaissa vaatimusta siitä, että tiedot ovat niihin oikeutettujen henkilöiden käytettävissä suunnitellulla tavalla.

[202] VM 2021:5, s. 25
[203] Mäenpää, 2008, s. 43
[204] Mäenpää, 2008, s. 44
[205] Voutilainen, 2006, s. 112

Saatavuudella hallinnon asiakkaan näkökulmasta varmistetaan viranomaisten hallussa oleviin tietoihin pääsy. Tällöin tiedon saatavuuden varmistaminen on julkisuuden toteutumisen kannalta välttämätön vaatimus[206]. Saatavuudella mahdollistetaan helposti saatava käsitys viranomaisen hallitsemista tietokokonaisuuksista sekä sen sisällöstä riippumatta tietojen tallennustavasta [207] . Tiedon saatavuuden suojaaminen tietoturvallisuustoimenpiteillä voidaan käsittää olevan olennainen julkisuusperiaatteen toteutumiselle viranomaistoiminnassa, kattaen asiakirjojen julkisuuden, salassapidon ja tietojen jakelun. Saatavuuden turvaamisella varmistetaan, että kansalaisilla on oikeus päästä viranomaisten hallussa oleviin tietoihin, tukien avoimuutta ja julkishallinnon demokraattista toimintaa. Käytettävyysvaatimus korostaa tiedon saavutettavuutta suunnitellulla tavalla, edistäen tehokasta tietovarantojen hyödyntämistä. Tiedon saatavuus on siten keskeinen tekijä, joka edistää tiedon avoimuutta ja yleistä käytettävyyttä.

Vuoden 1999 julkisuuslakia säädettäessä on hallituksen esityksessä korostettu tarvetta huolehtia tietojen eheydestä tietotekniikkaan liittyvien riskien vuoksi. [208] Yli kaksikymmentä vuotta myöhemmin onkin perusteltua väittää, ettei tietotekniikkaan liittyvät riskit eivät ole vähentynyt. Tiedon eheydellä varmistetaan viranomaisen hallitsemien tietoaineistojen virheettömyydestä, oikeellisuudesta sekä paikkansapitävyydestä. Tiedon eheys korostuu etenkin viranomaisen julkisissa rekistereissä[209], missä tiedon oikeellisuus on keskeinen rekisterin julkista luotettavuutta edistävä tekijä.[210]

Tiedon eheys näyttäytyy julkisuusperiaatteen toteutumisen kannalta elintärkeänä. Sillä varmistetaan, että julkisen hallinnon tuottama tieto on oikeellista. Tiedon oikeellisuudella avulla voidaan varmistua viranomaisen tietojen paikkansa pitävyydestä

[206] Mäenpää, 2020, s. 282
[207] Mäenpää, 2020, s. 282
[208] HE 30/1998 vp, s. 77.
[209] HE 30/1998 vp, s. 77: ”rekisterimerkinnöille on asetettu korostettu luotettavuusvaatimus.”
[210] Mäenpää, 2020, s. 283

jolla edistetään kansalaisten luottamusta hallintoon. Eheydellä on keskeinen asema myös edistäessä kansalaisten sekä tiedotusvälineiden mahdollisuutta valvoa viranomaisen toimintaa. Tällöin tiedon eheyden säilyessä kansalaiset voivat luottaa hallintoon ja osallistua aktiivisesti yhteiskunnalliseen keskusteluun ja päätöksentekoon.

Mikäli viranomaisen tuottama tieto ei ole oikeellista tai etenkään saatavilla, nousee kysymys siitä, onko perustuslain mukaisen julkisuuden todelliseen toteutumiseen mitään mahdollisuutta? Tällöin etenkin yksilön näkökulmasta tietoturvallisuustoimenpiteillä edistetään merkittävästi julkisuusperiaatteen mukainen yksilön oikeus yhteiskunnalliseen tietoon sekä laajemmin oikeus hyvään hallintoon.

Tiedon luottamuksellisuudesta voidaan varmistua rajoittamalla tiedon saatavuutta vain niiden saataville, jotka ovat oikeutettuja käsittelemään tietoa. Tiedon luottamuksellisuus osana julkisuuden toteuttamista nouseekin keskeiseen rooliin etenkin silloin, kun tiedon julkisuutta rajataan [211] . Hallituksen esityksessä koskien julkisuuslakia tiedon suojaamisella tarkoitetaan tiedon saatavuuden ja käyttötarkoituksia koskevien rajoitusten, kuten salassapidon ja henkilötietojen suojan toteuttamiseksi vaadittavia tarpeellisia toimenpiteitä [212] . Asiakirjojen turvallisuusluokkaa koskevalla merkinnällä osoitetaankin se, minkälaisia tietoturvallisuustoimenpiteitä tulee asiakirjaa käsitellessä noudattaa (TiHL 18 §). Tiedon suojaaminen tietoturvallisuustoimenpiteiden avulla voidaankin käsittää tosiasialliseksi toiminnaksi joka luo tiedolle luottamuksellisuuden.

Julkisuusperiaatteen turvaamisessa salassapitovelvoitteiden osalta luottamuksellisuuden tietoturvallisuusominaisuus nousee keskeiseen asemaan. Luottamuksellisuuden varmistaminen salassa pidetyissä tiedoissa tarkoittaa kuitenkin usein tiedon saatavuuden rajoittamista tietyltä osin. Tällöin tietoturvallisuutta toteuttaessa tulee kiinnittää erityistä huomiota erinäisten tietoturvallisuustoimenpiteiden väliseen oikeasuhtaiseen tasapainottamiseen.

[211] Mäenpää, 2020, s. 283
[212] HE 30/1998 vp, s. 77

Tietoturvallisuustoimenpiteitä suunnitellessa viranomaisen tulee huomioida julkisuuslainsäädännön velvoitteista koskien tietoja, joiden saatavuutta ja käytettävyyttä on lain mukaisin perustein rajattu. Etenkin salassa pidettävien tietojen käsittelyssä tiedon saatavuuden ja käytettävyyden rajoitukset tietoturvallisuustoimenpiteiden avulla edistävät julkisuuden tosiasiallista toteutumista.

Tietoturvallisuuden rooli julkisuusperiaatteen toteutumiselle on merkittävä. Tiedonhallinnan tietoturvallisuustoimenpiteitä suorittaessa viranomaisen on kyettävä varmistumaan tiedon laadullisista ominaisuuksista julkisuuden toteutumiseksi osana hyvää hallintoa. Tällöin tiedon eheys on kaiken lähtökohta, sillä sen avulla varmistutaan tietojen oikeellisuudesta. Yksilön kannalta huomiota tulee kiinnittää etenkin tiedon saatavuuteen, jolla turvataan keskeisesti yksilön pääsy yhteiskuntaa koskevaan tietoon.

5.3 Palveluperiaatteesta

Viranomaisten palveluntarjonta on nykyään pitkälti sähköistettyä, jolloin on varsin tavanomaista, että hallinnon asiakas ei fyysisesti kohtaa viranomaista hoitaakseen asioitaan. Sähköisen hyvän hallinnon palvelut toteutetaan pitkälti tietojärjestelmien avulla, jolloin tietoturvallisuus osana sähköisten palveluiden asianmukaista toimimista nousee keskeiseen asemaan. Tällöin tietoturvallisuuden ja sähköisen hyvän hallinnon suhdetta etenkin sähköisten palvelujen kannalta voidaan tarkistella hyvän hallinnon tunnusmerkistöön kuuluvan palveluperiaatteen kautta.

> *Asiointi ja asian käsittely viranomaisessa on pyrittävä järjestämään siten, että hallinnossa asioiva saa asianmukaisesti hallinnon palveluita ja viranomainen voi suorittaa tehtävänsä tuloksellisesti.*
>
> *Viranomaisen velvollisuudesta tiedottaa toiminnastaan ja palveluistaan sekä yksilöiden ja yhteisöjen oikeuksista ja velvollisuuksista toimialaansa liittyvissä asioissa säädetään viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 20 §:n 2 momentissa. (HaL 7§)*

Palveluperiaate asettaa kaksi erinäistä vaatimusta viranomaiselle. Ensinnä viranomaisen on pyrittävä järjestämään asiointi ja asian käsittely niin että hallinnon asiakas saa

asianmukaisesti hallinnon palveluita. Toisekseen viranomaisen tulee suorittaa tehtävänsä tuloksellisesti.[213] Viranomaisen tuloksellisella toiminnalla tarkoitetaan sitä, että asiointi tulisi voida tapahtua sekä hallinnossa asioivan että viranomaisen kannalta mahdollisimman nopeasti, joustavasti ja yksinkertaisesti sekä kustannuksia säätäen.[214] Palveluperiaatteen kontekstissa sen laatutaso sitoutuu hallintolain asianmukaisuuden vaatimukseen, jolloin viranomaisen kanssa asiointi ja asian käsittely tulee pyrkiä järjestämään mahdollisimman joustavaksi ja palvelumyönteiseksi. Asianmukaisuuden takaamiseksi keskeiseen asemaan asettuu palvelun saatavuus, laatu ja asiakkaan tarpeet.[215]

Tietoturvallisuuden asema viranomaisten digitaalisia asiointipalveluita sääntelevissä lakikokonaisuuksissa on saanut korostetun roolin. Tietoturvallisuuden takaaminen mainitaankin kaikissa digitaalisia palveluita sääntelevien lakikokonaisuuksien tavoitteissa.[216] Viranomaisen tiedonhallintaa sääntelevän tiedonhallintalain esitöissä on mainittu asiakaspalvelun kokonaisvaltaisen toimivuuden edellytykseksi viranomaisen taustajärjestelmien toimivuus[217]. Lisäksi digilain esitöissä on korostettu, että sähköisten asiointipalveluiden suunnittelussa ja tuotannossa on huomioitava palveluperiaatteesta kumpuavat velvollisuudet[218]. Yleisesti digitaalisten palveluiden sääntelyn tarkoituksena on turvata perustuslain 21 §:ssä säädetyt oikeusturvan ja hyvän hallinnon takeet hallinnon asiakkaan käyttäessä digitaalisia palveluita[219].

---

[213] Mäenpää, 2017, s. 272
[214] HE 72/2002 vp, s. 57
[215] Mäenpää, 2008, oikeus hyvään hallintoon, s. 78
[216] Voutilainen, 2023, s. 23–30. Voutilainen hahmottaa digitaalisten palveluiden kansallisen sääntelyn koostuvan Julkisuuslaista, tiedonhallintalaista, laista sähköisestä asioinnista viranomaistoiminnassa (13/2003, SAVL) ja laista digitaalisten palvelujen tarjoamisesta (306/2019, digipalvelulaki, DpL). Edellä mainituissa kahdessa viimeisessä lakikokonaisuudessa tietoturvallisuus mainitaan suoraa lain tarkoituksessa, ratio legis. Tiedonhallintalain tarkoituksena mainitaan julkisuuslainsäädännön toteutuminen.
[217] HE 284/2018 vp, s. 60, 123
[218] HE 60/2018 vp, s. 9
[219] Voutilainen, 2023, s. 27

5.4 Tietoturvallisuuden ominaisuuksien ja palveluperiaatteen suhteesta

Palveluperiaatteen asianmukaisuuden keskiössä digitaalisia palveluita toteuttaessa on etenkin palveluiden saatavuus. Valtion virastojen palvelujen saatavuus, mukaan lukien virastojen aukiolo- ja muut palveluajat, koskevat kaikkia ja liittyvät perustuslain 21 §:ssä säädettyyn jokaisen oikeuteen saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa[220]. Viranomaisen palvelujen saatavuudella mukaan lukien palveluajoilla on suoria vaikutuksia hallinnossa asioivan perustuslaissa suojattuun oikeuteen saada asiansa asianmukaisesti käsitellyksi[221]. Digitaalisia palveluita toteuttaessa palveluiden saatavuus ulottuu asiointipisteiden aukioloaikojen ulkopuolelle.

> *”Viranomaisen on huolehdittava sen vastuulla olevien digitaalisten palvelujen ja muiden viranomaisen käytössä olevien sähköisten tiedonsiirtomenetelmien saatavuudesta muulloinkin kuin viranomaisen asiointipisteiden aukioloaikoina.” (DpL 4 § 2 mom.)*

Digitaalisten palveluiden saatavuudesta huolehtiminen nähdään lainvalmisteluaineistossa osana tietoturvallisuusvaatimuksia [222] sekä digitaalisen palvelun teknistä toimivuutta [223] . Palveluperiaatteen mukaisella palveluiden saatavuudella ja tietoaineistoiden saatavuudella on sidoksensa [224], tosin niitä ei tule sekoittaa toisiinsa. Digitaalisten palveluiden saatavuutta kuvataan laissa saavutettavuudella, jolla tarkoitetaan periaatteita ja tekniikoita, joita on noudatettava digitaalisten palveluiden suunnittelussa, kehittämisessä, ylläpidossa ja päivittämisessä niin, että ne olisivat paremmin käyttäjien, erityisesti vammaisten saavutettavissa [225]. Saavutettavuus voidaan käsittää laajemmin osaksi käytettävyyttä, joka ulottuu

[220] HE 73/2022, s. 40-41
[221] HE 73/2022, s. 41
[222] HE 60/2018. s. 63
[223] HE 60/2018. s. 64
[224] Voutilainen, 2023, s. 283
[225] HE 73/2022, s. 10

laajemmin muun muassa viranomaisten digitaalisten palveluiden käyttöliittymien sääntelyyn[226].

Erinäiset tietoturvallisuuden laiminlyömisestä kumpuavat häiriötekijät voivat johtaa vakaviin ongelmiin, jotka estävät viranomaisen tuloksellisen toiminnan [227] . Tietoturvallisuudella lisätäänkin viranomaisen palvelukykyä sekä parannetaan tehokkuutta ja laatua, jolloin tietoturvallisuuden merkitys tuloksellisen toiminnan ylläpitämisessä on jatkuvasti korostunut [228]. Tietoturvallisuustoimenpiteillä on tällöin merkittävä rooli palveluperiaatteen mukaisen asianmukaisuuden sekä tehtävien tuloksellisen hoitamisen edistämiseksi. Tietoturvallisuustoimenpiteitä toteuttaessa on kuitenkin otettava huomioon niiden vaikutukset palveluperiaatteen mukaisen toiminnan edistämiseksi. Lainvalmisteluaineistossa onkin kiinnitetty huomiota siihen, miten tarpeettoman raskailla tietoturvallisuustoimenpiteillä voi olla kielteinen vaikutus viranomaisen toimintaan hidastaen työvaiheita [229] . Tällöin viranomaisen perusteettomilla tietoturvallisuustoimenpiteillä voi olla negatiivisia vaikutuksia viranomaisen sisäisten järjestelmien toimivuuteen ja nopeuteen hidastaen viranomaisen asiankäsittelyä perusteettomasti, jolloin perustuslain 21 §:n mukainen oikeus saada asiansa käsitellyksi ilman aiheetonta viivytystä saattaa vahingoittua. Myös hallinnon asiakkaan oikeus saattaa asiansa käsitellyksi asianmukaisesti perustuslain 21 §:n mukaisesti voi estyä, mikäli tietoturvallisuustoimenpiteet ovat hallinnon asiakkaalle tarpeettoman raskaat tai vaativat erityistä tietotaitoa mitä ei voida palvelun käyttäjältä odottaa.

Tietoturvallisuuden rooli hyvän hallinnon palveluperiaatteen mukaisen palveluiden asianmukaisuuden ja viranomaisen tuloksellisen toiminnan takaamisessa on perustellusti merkittävä. Etenkin digitaalisten palveluiden osalta tietoturvallisuustoimenpiteillä mahdollistetaan palveluiden jatkuva saatavuus, joka

[226]Ks. lisää Koulu ja muut käytettävyyden ulottuvuuksista osana digitaalisen hallinnon saatavuutta.
[227] VAHTI 2/2004, s. 9
[228] VAHTI 2/2004, s. 5
[229] HE 17/2002 vp, s. 28

käsitetään keskeiseksi osaksi asianmukaisuutta. Mikäli viranomaisen digitaalinen palvelu on kohtuuttoman pitkän aikaa alhaalla esimerkiksi palvelunestohyökkäyksen takia, on mahdollista, että hallinnon asiakas ei saa perustuslain 21 §:n mukaisesti saatettua asiaansa vireille toimivaltaisessa viranomaisessa hyvän hallinnon säännöstön mukaisesti. Vastaavasti viranomaisten omien taustatietojärjestelmien toimimattomuus tietoturvallisuusongelmista kumpuavista syistä voi johtaa asiankäsittelyn viivästymiseen sekä viranomaisen oman toiminnan nopeuteen ja joustavuuteen, vaikuttaen kielteisesti viranomaisen toiminnan tuloksellisuuteen.

5.5 Viranomaisten yhteistyö

Hallintolaissa esiintyvien muiden hyvän hallinnon perusteiden ja tietoturvallisuuden välistä suhdetta on syytä tarkastella tarkemmin. Viranomaisten välisestä yhteistyöstä säädetään hallintolain 10 §:ssä.

> *”Viranomaisen on toimivaltansa rajoissa ja asian vaatimassa laajuudessa avustettava toista viranomaista tämän pyynnöstä hallintotehtävän hoitamisessa sekä muutoinkin pyrittävä edistämään viranomaisten välistä yhteistyötä.” (HL 10 § 1 mom.)”*

Viranomaisten välisellä yhteistyöllä on vahva sidos hallinnon asiakkaan asianmukaisen palvelun saannin kannalta. Yhteistyöllä mahdollistetaankin se, että asiakkaan ei pidä asioida jokaisen viranomaisen kanssa erikseen. Lisäksi viranomaisten välinen yhteistyö edistää asian selvittämistä ja valmistelua liittyvää toimintaa, jossa keskiössä on tietojen tehokas ja joustava välittäminen.[230] Viranomaisten välistä yhteistyötä rajoittaa kuitenkin tiedon luottamuksellisuus salassapidon osalta. Yhteistyössä tulee huomioida julkisuuslain 29 §:n säädös salassa pidettävien tietojen antamisesta toiselle viranomaiselle[231]. Viranomaisten välisen yhteistyön toimivuudella on keskeinen rooli hallintoasian selvittämisessä sekä yleisesti hallinnon toimivuuden kannalta. Tehokas viranomaisyhteistyö edistää asioinnin helppoutta ja sillä voidaan saavuttaa tuloksia,

[230] Mäenpää, 2023, s. 259
[231] Mäenpää, 2023, s. 260

joihin viranomainen ei yksittäisillä toimenpiteillään välttämättä pääse.[232] Tehokkaalla ja asianmukaisella viranomaisyhteistyöllä parannetaan hallintotoiminnan laatua ja sen tehokkuutta sekä mahdollistetaan parempi hallinnossa asioivien palvelu [233] . Laillisuusvalvonnassa onkin katsottu viranomaisen välisellä yhteistyöllä olevan varsin keskeinen merkitys hyvän hallinnon takeiden toteutumisen näkökulmasta[234].

Viranomaisten välinen yhteistyö perustuu laajalti tietojen vaihtoon, jolloin tiedon laadullisten ominaisuuksien turvaaminen yhteistyön toimivuuden takaamiseksi on nähtävissä keskeisessä asemassa. Käytettävyyden käsitteeseen yhdistetään vaatimus huolehtia muiden viranomaisten tiedonsaantitarpeiden huomioon ottamisesta silloin, kun toinen viranomainen on riippuvainen muualta saatavasta tiedosta [235] . Tällöin tietoturvallisuustoimenpiteillä varmistettava tietojen ominaisuuksien turvaaminen saa huomattavan painoarvon edistäessä hallintolain 10 §:n ja laajemmin hyvän hallinnon mukaista viranomaisten välistä yhteistyötä. Tietojen ollessa asianmukaisesti suojattu viranomainen voi luottaa siihen, että jaettu tieto säilyy luottamuksellisena ja suojattuna. Tietoturvallisuustoimenpiteillä varmistetaan tietojen eheys ja oikeellisuus, joka edesauttaa välttämään tietojen vääristymistä tai tahallista manipulointia, mikä on olennaista yhteistyön toimivuuden kannalta. Tietoturvalliset järjestelmät ja käytännöt mahdollistavat turvallisen tiedonvaihdon ja saatavuuden eri viranomaisten välillä edistäen sujuvaa ja tehokasta yhteistyötä eri viranomaisten välillä. Hyvällä tietoturvallisuuskulttuurin ylläpitämisellä voi olla myös luottamusta edistävä rooli, jolloin viranomaiset voivat luottaa siihen, että jaettu tieto on asianmukaisesti suojattu edistäen yhteistyön ilmapiiriä. Edellä mainittujen yhteisvaikutus edesauttaa varmistamaan, että viranomaisten välillä on vahva perusta luottamukselliselle, tehokkaalle ja lainmukaiselle yhteistyölle hallintolain 10 §:n edellyttämällä tavalla.

[232] HE 72/2002 vp, s. 65
[233] Mäenpää, 2021, s. 225
[234] AOKVM/ 849/1/97
[235] HE 30/1998 vp, s. 77

5.6 Viranomaisen neuvonta

Viranomaisen neuvontavelvollisuudesta säädetään hallintolain 8 §:ssä osana hyvän hallinnon perusteita.

> *”Viranomaisen on toimivaltansa rajoissa annettava asiakkailleen tarpeen mukaan hallintoasian hoitamiseen liittyvää neuvontaa sekä vastattava asiointia koskeviin kysymyksiin ja tiedusteluihin. Neuvonta on maksutonta.*
>
> *Jos asia ei kuulu viranomaisen toimivaltaan, sen on pyrittävä opastamaan asiakas toimivaltaiseen viranomaiseen.” (HaL 8 §)*

Neuvonnalla tarkoitetaan asian vireillepanoon ja käsittelyyn liittyvien neuvojen antamista sekä vastaamista asiakkaan kysymyksiin ja tiedusteluihin sekä viranomaisen antama opastus, jonka tarkoituksena on löytää toimivaltainen viranomainen. Viranomaisen neuvontavelvollisuus koskee kaikkia hallintoasian käsittelyvaiheita sekä sen hoitamiseksi liittyvää toimintaa.[236] Neuvonnan pääpaino on tilannekohtaisessa neuvonnassa, jota voidaan täydentää yleisellä tiedottamisella. Hallinnon asiakkaan oikeussuojan kannalta keskeisiä arviointiperusteita neuvonnan kannalta ovat sen laajuus, riittävyys ja virheettömyys. Neuvonnalla pyritään siihen, että henkilö pystyy hoitamaan asiansa itse. Viranomaisen tulee vastata asiointia koskeviin tiedusteluihin ja kysymyksiin kohtuullisessa ajassa sekä pyrkiä oikaisemaan asiakkaan väärinkäsityksen oma-aloitteisesti.[237]

Viranomaisen neuvonnassa tulee tietoturvallisuuteen kiinnittää huomiota etenkin käsitellessä salassa pidettäviä tietoja. Laillisuusvalvonnassa on usein kiinnitetty huomiota salassa pidettävien tietojen lähettämisestä suojaamattomassa sähköpostissa[238]. Suojaamattoman sähköpostiyhteyden kautta voidaan antaa yleistä neuvontaa, kuten etuuksien hakemiseen liittyviä ohjeita. Mikäli tiedusteluun ei voida

---

[236] Mäenpää, 2021, s. 214-215
[237] Kulla & Salminen. 2021. s.139-140
[238] Viranomainen ei voi lähettää salassa pidettäviä tietoja suojaamattomassa sähköpostissa. Ks. OKV/1913/1/2018, OKV/1964/1/2017, OKV/96/1/2016, OKV/1131/1/2013, EOA/3438/4/2009

vastata paljastamatta asiakkaan nimeä tai muita asiakastietoja, tulee tiedusteluun vastata puhelimella tai kirjallisesti.[239] Kun kyseessä on salassa pidettävien tietojen käsittely, on tietoturvallisuudella eittämättä keskeinen asema niin tietojen kun tiedonsiirtokanavien turvaamiseksi.

Teknologian ja etenkin tekoälyn kehittyessä on viranomaisen neuvonta saanut uusia ulottuvuuksia. Kehitys on mahdollistanut erinäisten chatbot-sovellusten implementoinnin osaksi viranomaisen neuvontapalveluita. Chatbot-sovelluksien antama neuvonta on yhtälailla viranomaisen neuvontaa siinä missä virkasuhteessa olevan luonnollisen henkilön antama neuvonta. Erityistä siitä tekee tavanomaiseen neuvontaan se, että käyttäessä chatbot-sovellusta hallinnon asiakas ei saa neuvontaa luonnolliselta henkilöltä. Chatbot-sovelluksen neuvonta perustuukin pitkälti tietokoneohjelman algoritmien käsittelemään viranomaisen tietoaineistoon[240].

Tällöin etenkin viranomaisen tietoaineiston eheys nousee keskeiseen asemaan osana viranomaisen chatbot-sovelluksia, sillä sovelluksen tuottama neuvonta perustuu sille ennalta annettuun tietoaineistoon. Mikäli sen käyttämä tietoaineisto ei ole oikeellista, on hyvinkin mahdollista, että hallinnon asiakkaan saama neuvonta ei täytä hyvän hallinnon vaatimuksia neuvonnan asianmukaisuudesta ja laadusta. Lisäksi chatbot-sovelluksien algoritmien koodeihin liittyvät ongelmat voivat myös luoda tiedon luottamuksellisuuden vaarantavia ongelmia, mikäli ne eivät toimi määritellyllä tavalla. Tällöin voi olla mahdollista, että chatbot-sovellus antaa neuvonnan yhteydessä tietoja viranomaisen tietoaineistosta mihin asiakas ei välttämättä ole oikeutettu.

5.7 Tietoturvallisuudesta perusoikeutena

Suomalaisessa oikeuskirjallisuudessa tietoturvallisuutta on käsitelty ensisijaisesti metaoikeutena ja metaperiaatteena[241]. Tietoturvallisuuden hahmottaminen

[239] TSV 1.7.2010
[240] Voutilainen, 2008, s. 913
[241] Ks. 2. luku metaperiaatteista

oikeustieteessä metaperiaatteeksi tai jopa metaoikeudeksi on vahva argumentti perusteltaessa tietoturvallisuuden oikeudellista merkitystä. Tietoturvallisuus ilmenee perusoikeuksiemme välttämättömäksi edellytykseksi. [242] Verkkoyhteiskunnassa useat perusoikeudet ovat riippuvaisia tietoturvallisuudesta, jolloin nousee kysymys tietoturvallisuuden asemasta perusoikeutena. Tietoturvallisuudesta perusoikeutena ei ole kuitenkaan suoranaista mainintaa lainsäädännössä, vaikka se oikeustieteessä nähdään merkittävänä metaperiaatteena.

Tietoturvallisuusriippuvaisiksi perusoikeuksiksi on oikeuskirjallisuudessa nähty kuuluvan oikeus henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen (PeL 7 §), yksityiselämän, kunnian ja henkilötietojen suoja (PeL 10 §), luottamuksellisen viestin ja salaisuuden loukkaamattomuuden (PeL 10 §:n 2 mom.), sananvapaus sekä viranomaisten asiakirjojen ja tallenteiden julkisuus (PeL 12 §), omaisuuden suoja (PeL 15 §) ja oikeusturva, jonka sisältöön kuuluvat asian joutuisan käsittelyn ja hyvän hallinnon takeet (PeL 21 §)[243].

Perustuslain 7 §:n mukaisesti jokaisella on oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen. Oikeus turvallisuuteen on yleisesti käsitetty osaksi henkilökohtaisen vapauden ja koskemattomuuden suojaan käsitettävänä oikeutena, missä oikeus henkilökohtaiseen turvallisuuteen takaa yksilöön kohdistuvan mielivaltaisen puuttumisen henkilökohtaiseen vapauteen sekä koskemattomuuteen. Oikeutta turvallisuuteen ei siis nähdä itsenäisenä perusoikeutena, vaan turvallisuuden mainitsemisella korostetaan julkisen vallan positiivista toimintavelvoitetta yhteiskunnan jäsenten suojaamiseksi rikoksilta ja muilta heihin kohdistuvilta oikeudenvastaisilta teoilta, riippumatta onko tekijät julkisen vallan käyttäjiä tai yksityisiä toimijoita. [244] Henkilökohtainen turvallisuus käsiteteenäkin perinteisesti koskevan fyysistä turvallisuutta.

---

[242] Råman, 2006, s. 818-819
[243] Pöysti & Saarenpää. 1997, s. ixii. Ja Saarenpää & Wiatrowski, 2016, s. 237
[244] HE 309/1993 vp, s. 47

Råman (2006) onkin esittänyt turvallisuusperusoikeuden kytkennän fyysiseen turvallisuuteen olevan jäänne erilaisesta yhteiskunnasta, jolloin informaatiolla, luottamuksellisen viestin sekä yksityisyyden suojalla ei ole ollut samaa merkityssisältöä kuin nykyään. Råman näkee tietoturvallisuuden niin merkittävänä osana yksilön toimintaa ja oikeuksien käyttöä verkkoyhteiskunnassa, että se tulisi lukea osaksi perutuslain 7 §:n 1 momenttia. [245] Tietoturvallisuudella voi lisäksi olla fyysiseen turvallisuuteen liittyviäkin aspekteja, esimerkiksi salausvirheessä, jolloin henkilön uusi nimi tai olinpaikka voi paljastua lähestymiskiellon saaneelle henkilölle. Myös erinäisissä sairaanhoidon [246] järjestelmien ja laitteiden tietoturvallisuuspuutteilla voi olla suoranaisia vaikutuksia yksilön fyysiseen turvallisuuteen. Myös perustuslakivaliokunta on lausunnossaan todennut, että tietoturvallisuuden vaarantumista voidaan nykyaikana pitää riskinä yksilön ja yhteiskunnan turvallisuuden kannalta [247]. Euroopan unionin verkko- ja tietoturvallisuutta käsittelevässä NSI-direktiivissä (EU 2016/1148) korkeatasoinen verkko- ja tietoturvallisuus nähdään yhtenä modernin turvallisuuden keskeisenä elementtinä.

Euroopan ihmisoikeustuomioistuimen ratkaisun (EIT 17.7.2008 20511/03, I. vastaan Suomi) on käsitelty tietoturvallisuuden ja yksityiselämän suojan välistä yhteyttä. Tapauksessa oli kyse sairaalan potilastietojen käsittelystä ja niiden päätymisestä ulkopuolisille henkilöille sekä potilastietojärjestelmän pääsynhallinnasta. Ratkaisun mukaisesti tuomioistuin katsoi, että potilastietojärjestelmän tietoja oli päätynyt sellaisten henkilöiden käsiin, joilla ei ole ollut oikeutta käsitellä tietoja loukaten Euroopan ihmisoikeussopimuksen 8 artiklan 1 kohdassa säädettyä yksityiselämän suojaa. Tuomioistuin korostaa päätöksessä valtion positiivista velvollisuutta huolehtia tietojärjestelmissä olevien yksityiselämän suojan piiriin kuuluvien tietojen suojaamisesta ja turvaamisesta lainsäädäntötasolla sekä asianmukaisin tietoturvallisuustoimenpitein.

[245] Råman, 2006, s. 819
[246] Ks. D. Halperin ja muut. (2008).
[247] PeVL 9/2004 vp, s. 4

Ratkaisun valossa tietoturvallisuus näyttäytyy merkittävänä tekijänä turvatessa etenkin yksityiselämän suojan toteutumista. Lisäksi tuomioistuimen näkemys valtion velvollisuudesta vaikuttaa positiivisesti tietoturvallisuuden toteutumiseksi, on sillä nähtävissä olevan sidos ihmisoikeuksien toteutumiseen.

Perustuslain 22 §:n mukaan julkisen vallan on turvattava perus- ja ihmisoikeuksien toteutuminen. Vaikka tietoturvallisuudesta perusoikeutena ei suoranaisesti säädetä perustuslaissa, on nähdäkseni kuitenkin perustuslain asettaman perus- ja ihmisoikeuksien turvaamisvelvollisuudesta sekä kansallisessa lainsäädännössä esiintyvien tietoturvallisuusvelvoitteiden ja tietoturvallisuussääntelyn välillä löydettävissä merkittävä yhteys tietoturvallisuuden ja perusoikeuksien toteutumisen välille.

6 Johtopäätökset

Digitalisaation vaikutuksesta tietokoneet, tietojärjestelmät ja tietoverkot ovat mahdollistaneet ennenäkemättömällä tavalla käsitellä tietoa. Samaan aikaan hallinto on tullut näistä teknologisista toiminnoista eittämättä riippuvaiseksi kauttaaltaan jokapäiväisessä toiminnassaan. Viranomaisaineistojen sisältävät tietovarannot ja niiden tietoturvallisuus onkin noussut keskeiseen asemaan verkkoyhteiskunnassa, joka on johtanut tarpeeseen säätää tietoturvallisuudesta lain tasolla uudessa sähköisessä toimintaympäristössä. Perinteisten oikeuksien toteutuminen sähköisessä ympäristössä ja vallitsevien lakien yhteensovittaminen onkin osoittautunut jossain määrin haastavaksi, sillä ne kumpuavat ajalta ennen digitaalista maailmaa.

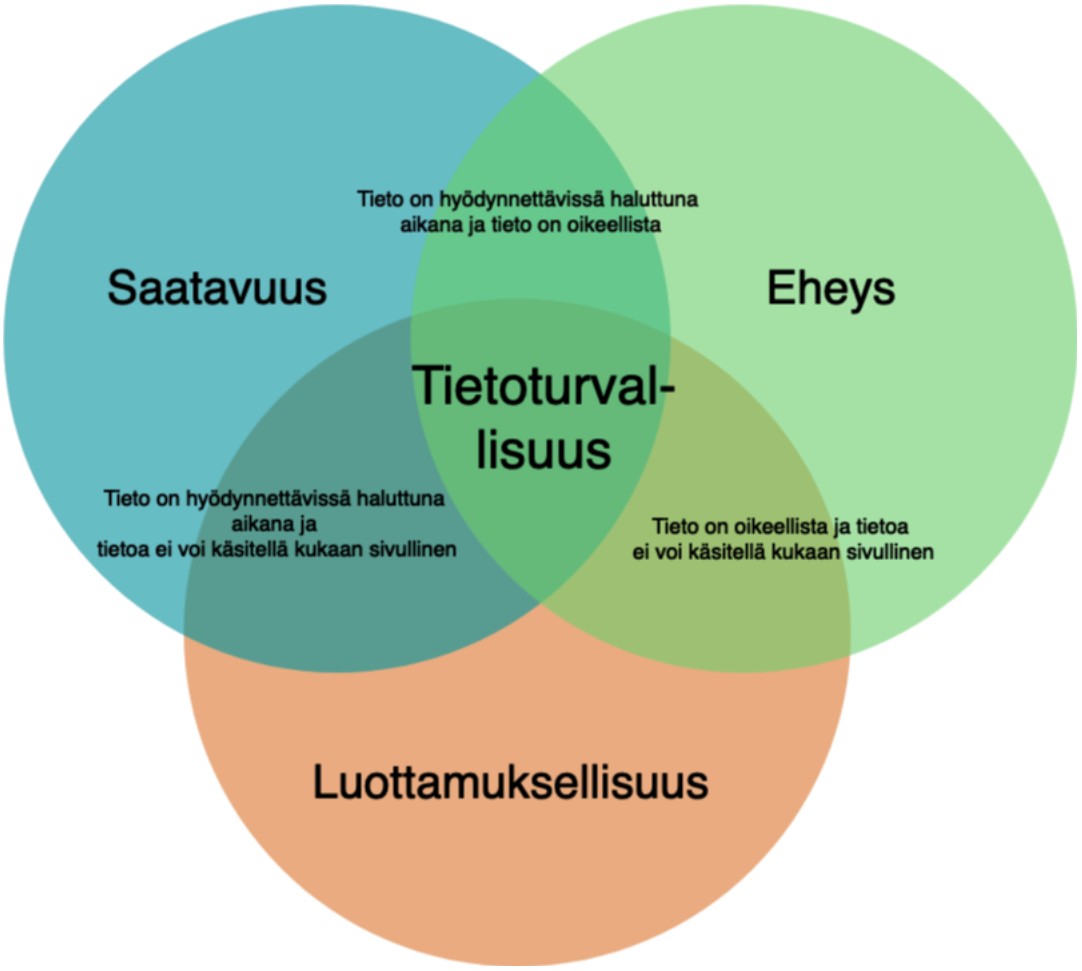
Digitaalisen maailman tietoturvallisuuden toteuttaminen teknisin toimenpitein jää usein tietotekniikan ja tietojenkäsittelytieteiden alaisuuteen. Tästä syystä tietoturvallisuuden oikeustieteellisessä kontekstissa ei puututa niinkään sen teknisiin toteutustapoihin ja toimenpiteisiin, vaan oikeustieteelle jää pikemminkin sen arviointi täyttääkö tietojärjestelmä, ohjelmisto tai muu tietotekninen ratkaisu lain vaatimat edellytykset. Lisäksi oikeustieteellä, etenkin informaatio-oikeudella on keskeinen rooli tutkiessa informaation ja tiedon suojaamisen oikeudellisen sääntelyn tarvetta sekä mahdollisuuksia.

Tämän tutkielman ensimmäisenä tutkimuskysymyksenä oli, miten kansallinen lainsäädäntö velvoittaa viranomaista huolehtimaan tietoturvallisuudesta sekä mistä tietoturvallisuus oikeudellisena käsitteenä koostuu? Toisena tutkimuskysymyksenä oli millaisen käsitesisällön sekä roolin tietoturvallisuus saa osana hyvän hallinnon tunnusmerkistöä sekä laajemmin mahdollisena perusoikeutena?

Tietoturvallisuus oikeudellisena käsitteenä sisältää pitkän historiansa aikana monia erilaisia ilmenemismuotoja, joka on muokkaantunut historian saatossa etenkin teknisen kehityksen ja digitalisaation myötä. Tietoturvallisuuden oikeudellisen käsitteen sisältöä hahmottamisessa tulee huomioida ensinnäkin sen rooli oikeusperiaatteena ja

mahdollisena metaoikeutena. Tietoturvallisuuden hahmottaminen oikeudellisena käsitteenä kiteytyy kolmeen keskeiseen tiedon ominaisuuteen: tiedon saatavuuteen, eheyteen ja luottamuksellisuuteen. Nämä kolme tiedon ominaisuutta muodostavat kokonaisuuden, jolla taataan tietojärjestelmien ja tietoaineistojen asianmukainen suoja. Saatavuuden, eheyden ja luottamuksellisuuden ominaisuudet esiintyvät tietoturvallisuuden oikeudellisen käsitteen lähtökohdiksi kauttaaltaan aineistossa. Edellä mainitut ominaisuudet ovat keskeisiä arvioidessa tietoturvallisuutta, olipa kyse sitten tietojärjestelmistä, tietoverkoista tai itse tiedoista, ja ne muodostavat perustan luotettavalle ja turvalliselle tietojenkäsittelylle.

Saatavuudella varmistetaan, että tarvittavat tiedot ovat saatavilla oikeille ihmisille oikeaan aikaan ilman viivettä tai häiriöitä. Eheydellä varmistetaan, että tiedot pysyvät muuttumattomina, luotettavina ja alkuperäisinä koko niiden käsittelyn ajan. Luottamuksellisuudella käsitetään, että arkaluontoiset tiedot ovat suojattuja ja niitä pääsevät käyttämään vain oikeutetut henkilöt. Tiedon ominaisuudet ovat toisiinsa vahvasti vuorovaikutussuhteessa olevia käsitteitä, joita tulee tietoturvallisuuden saavuttamiseksi käsitellä kokonaisuutena eikä yksittäisinä osatekijöinä. Yhden ominaisuuden turvaaminen ei siis vielä takaa tietoturvallisuuden kokonaisvaltaista toteutumista, vaan kaikki tiedon kolme ominaisuutta tulee turvata kauttaaltaan. Tietoturvallisuuden ja sen ominaisuuksien välistä suhdetta voidaan hahmottaa seuraavasti.



Kuvio 1. Tiedon ominaisuuksien suhde tietoturvallisuuteen

Viranomaisen velvollisuus huolehtia tietoturvallisuudesta saa maininnan useassa lakikokonaisuudessa. Tietoturvallisuudesta säädetään yleislain tasolla tiedonhallintalain neljännessä kappaleessa, jonka säädökset käsittelevät viranomaisen velvollisuuksista huolehtia tietoturvasta. Tiedonhallintalain tietoturvallisuussääntelyn keskiössä ovat tietoturvallisuustoimenpiteet, jolla tarkoitetaan erinäisiä hallinnollisia, toiminnallisia ja teknisiä toimenpiteitä tietoturvallisuuden saavuttamiseksi. Tietoturvallisuustoimenpiteet ovatkin niitä konkreettisia tekoja, joilla suojataan tietoa.

Tiedonhallintalaista kumpuavat viranomaiselle asetetut velvoitteet tietoturvallisuuden huolehtimisesta perustuvat riskipohjaiseen suunnitteluun, jossa tietoturvallisuustoimenpiteiden laajuus suhteutetaan mahdollisten uhkien vakavuuteen.

Tiedonhallintalain säädökset muodostavat sääntelykokonaisuuden joka ottaa huomioon tietoturvallisuuden eri osa-alueet tiedon ominaisuuksien suojaamiseksi. Tietoturvallisuuden järjestämisen vastuu viranomaisen organisaatioissa kohdistuu tiedonhallintayksikön johdolle. Tiedonhallintayksikölle säädettyjä tiedonhallintaan ja tietoturvallisuuteen liittyviä menettelytapoja ja vaatimuksia arvioi sekä edistää itsenäisenä viranomaisena toimiva tiedonhallintalautakunta.

Hyvän hallinnon ja tietoturvallisuuden välistä suhdetta etsiessä nousi keskeiseksi hyvän hallinnon moninaisuus. Hyvä hallinto voidaan nähdä kattokäsitteenä, joka pitää sisällään useita erinäisiä vaatimuksia siitä, mikä käsitetään hyväksi hallinnoksi. Tutkielmassa on keskitytty hahmottamaan tietoturvallisuuden suhdetta perustuslain 21 §:n ja hallintolain 2 luvun mukaisten hyvän hallinnon osatekijöiden pohjalta. Keskeisenä näistä on ollut varsinkin tietoturvallisuuden suhde julkisuusperiaatteen, palveluperiaatteen, viranomaisten yhteistyön ja neuvonnan toteutumiseen.

Julkisuusperiaatteen yhteydessä tietoturvallisuus näyttäytyy elintärkeänä. Tietoturvallisuudella taataan viranomaisten tuottaman ja hallinnoiman tiedon oikeellisuus. Tietotuvallisuudella lisäksi mahdollistetaan kansalaisten mahdollisuus päästä käsiksi viranomaisten tietoihin, joka on keskeinen vaatimus julkisuusperiaatteen toteutumiselle. Lisäksi tiedon luottamuksellisuudella varmistetaan, että viranomaisten tiedot päätyvät vain niiden käsiteltäväksi, joilla on siihen salassapitovelvoitteiden mukainen oikeus.

Palveluperiaatteen ja tietoturvallisuuden välisessä suhteessa keskiöön nousee hallinnon asiakkaan oikeus saada hallinnon palveluita asianmukaisesti sekä viranomaisen toiminnan tuloksellisuuden vaatimus. Tietoturvallisuuden rooli viranomaisen tuloksellisessa toiminnassa näyttäytyy verkkoyhteiskunnassa kiistämättä merkittävänä. Digitalisaation aikaan saama tekninen kehitys on edistänyt viranomaisen tuloksellisuutta huomattavasti, jolloin tietoturvallisuustoimenpiteet mahdollistavat näiden teknologisten ratkaisujen häiriöttömän toiminnan. Tällä on suora vaikutus myös

hallinnon asiakkaan oikeuteen saada asianmukaista palvelua etenkin viranomaisten digitaalisissa palveluissa.

Tietoturvallisuudella osana viranomaisten välistä yhteistyötä on nähtävissä yhteyksiä palveluperiaatteen mukaiseen toiminnan tuloksellisuuteen sekä palveluiden asianmukaisuuteen. Tietoturvallisuustoimenpiteillä järjestetty viranomaisten välinen tietoturvallinen tietojenvaihto mahdollistaa viranomaisten toiminnan tuloksellisuuden ja tehokkaan toiminnan. Mikäli tiedot eivät ole saatavilla viranomaisten välillä tai niiden toimittaminen ei ole tietoturvallista viranomaisten välillä on mahdollista, että viranomaisen oma toiminta hidastuu merkittävästi vaikuttaen kielteisesti asian käsittelyn asianmukaisuuteen.

Tietoturvallisuus näyttäytyy merkittävänä tekijänä osana hyvän hallinnon toteutumista. Laajemmin tietoturvallisuus on nähtävissä usean eri perusoikeuden toteuttajana. Sen perusoikeusasemaa voidaan hahmottaa muiden perusoikeuksien kautta niiden tietynlaisena taustatoteuttajana sekä sen metaoikeudellisen aseman valossa. Itsenäisenä perusoikeutena sitä ei kuitenkaan nykyisessä lainsäädännössä nähdä, tosin verkkoyhteiskunnan kehittyessä ja turvallisuuden käsityksen muokkautuessa ajan saatossa tilanne voi olla täysin toinen tulevaisuudessa.

Lähteet

Virallislähteet

HE 284/2018 vp. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.

HE 30/1998 vp. Hallituksen esitys Eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi.

HE 60/2018 vp. Hallituksen esitys eduskunnalle laeiksi digitaalisten palvelujen tarjoamisesta sekä sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta.

HE 284/2018 vp. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.

HE 72/2002 vp. Hallituksen esitys eduskunnalle hallintolaiksi ja laiksi hallintolainkäyttölain muuttamisesta.

HE 17/2002 vp. Hallituksen esitys eduskunnalle laiksi sähköisestä asioinnista viranomaistoiminnassa.

HE 73/2022 vp. Hallituksen esitys eduskunnalle laeiksi valtion palveluiden saatavuuden ja toimintojen sijoittamisen perusteista annetun lain ja julkisen hallinnon yhteispalvelusta annetun lain 2 §:n muuttamisesta.

HE 309/1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

ITU. International Telecommunication Union. internet security threat report 2015. Noudettu 30.11.2023: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf

KHO. (2019). Korkeimman hallinto-oikeuden asiantuntujalausunto hallituksen esityksestä HE 284/2019 vp.

LVM 2021:7. (2021). Liikenne- ja viestintäministeriö. Kyberturvallisuuden kehittämisohjelma.

PeVL 7/2019 vp. Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle laiksi henkilötietojen käsittelystä maahanmuuttohallinnossa ja eräiksi siihen liittyviksi laeiksi.

PeVL 9/2004 vp. Perustuslakivaliokunnan lausunto hallituksen esityksestä sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi.

HaVM 38/2018 vp. (2018). Hallintovaliokunnan mietintö hallituksen esityksestä eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.

VAHTI 22/2017 Valtiovarainministeriö. (2017). Ohje riskienhallintaan. ISBN 978-952-251-862-0

VAHTI 8/2008 Valtiovarainministeriö. (2008). Valtionhallinnon tietoturvasanasto. ISBN 978-951-804-889-6.

VAHTI 2/2008 Valtiovarainministeriö. (2008). Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. ISBN 978-951-804-799-8

VAHTI 3/2007 Valtiovarainministeriö. (2007). Tietoturvallisuudella tuloksia. ISBN 978-951-804-768-4

VAHTI 2/2004 Valtiovarainministeriö. (2004). Tietoturvallisuus ja tulosohjaus. ISBN 951-804-432-5

VM 2020:18 Valtiovaranministeriö. (2020). Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa.

VM 2022:8 Valtiovarainministeriö. (2022). Tiedonhallintalautakunnan arviointikertomus 2020-2021

VM 2022:43. Valtiovarainministeriö. (2022). Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) – suositus ja kriteeristö. ISBN 978-952-367-275-8

VM 2021:65. Valtiovarainministeriö. (2021). Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. ISBN 978-952-367-897-2

VM 2021:5. Valtiovarainministeriö. (2021). Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

VM 2020:53. Valtiovarainministeriö. (2020). Suositus tiedonhallinnan muutosvaikutusten arvioinnista. ISBN 978-952-367-318-2

VM 2020:29. Valtiovarainministeriö. (2020). Suositus tiedonhallintamallista. ISBN 978-952-367-328-1

VM 2020:23. Valtiovarainministeriö. (2020). Julkisen hallinnon digitaalinen turvallisuus. http://urn.fi/URN:ISBN:978-952-287-857-1

VM/2500/00.01.00.01/2017. Valtiovarainministeriö. (2017). Asettamispäätös: Julkisen hallinnon tiedonhallintalain valmistelu.

VM 2000:11. Valtiovarainministeriö. (2000). Hyvän tiedonhallintatavan määritys. ISBN 951-804-164-4

VN 2019:31. Valtioneuvosto. (2019) Pääministeri Sanna Marinin hallituksen ohjelma 10.12.2019. Osallistuva ja osaava Suomi – sosiaalisesti, taloudellisesti ja ekologisesti kestävä yhteiskunta.

VN 2023:58. Valtioneuvosto. (2023). Pääministeri Petteri Orpon hallituksen ohjelma 20.6.2023. Vahva ja välittävä Suomi.

LVM 2021:1 Liikenne- ja viestintäministeriö. (2020). Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Työryhmän loppuraportti.

LVM/2021/44 Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla.

Kansallinen turvallisuusviranomainen (Traficom). (2020). Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille. ISBN 2669-8757

Parviainen, Päivi. Kääriäinen, Jukka. Honkatukia, Juha. Federley, Maija. (2017). Julkishallinnon digitalisaatio – tuottavuus ja hyötyjen mittaaminen. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 3/2017.

COM(2003) 567 final. The Role of eGovernment for Europe's Future. Communication from the commission to the council, the european parliament, the european economic and social committee and the committee of the regions.

Laillisuusvalvonta

AOKVM 26.02.1998. Dnro 849/1/97. Asian käsittelyn viivästyminen.

EOA 24.3.2009. Dnro 3438/4/2009. Salassa pidettäviä tietoja ei saa lähettää suojaamattomassa sähköpostissa.

OKV 9.12.2019. Dnro 1913/1/2018. Salassa pidettävien tietojen lähettäminen suojaamattomassa sähköpostissa.

OKV 6.3.2018. Dnro 1964/1/2017. Käsittelyn asianmukaisuus ja viipyminen.

OKV 27.4.2016. Dnro 96/1/2016. Salassa pidettävien tietojen lähettäminen suojaamattomassa sähköpostissa

OKV 11.11.2014. Dnro 1131/1/2013. Salassa pidettävien tietojen lähettäminen suojaamattomassa sähköpostissa

OKV 28.4.2014. Dnro 1242/1/2013. Virheellisten tietojen luovuttaminen

EAO 12.8.2010. Dnro 537/4/10. Käräjäoikeuden sähköpostijärjestelmän englanninkielinen virheilmoitus

TSV 1.7.2010. Dnro 1475/41/2009. Sähköpostin ja tekstiviestien käyttäminen terveydenhuollossa.

Tuomioistuinten ratkaisut

EIT 20511/03 I v. Finland (17.7.2008)

Kirjallisuus

Aarnio, Aulis (1989). Laintulkinnan teoria. Werner Söderström Osakeyhtiö, Porvoo Helsinki–Juva.

Aarnio, Aulis: Tulkinnan taito: Ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. Talentum Media, Helsinki 2006.

Alexy, Robert. (2000). On the Structure of Legal Principles. Ratio Juris. Vol. 13 No. 3 September 2000.

Andersson, Ari & Koivisto, Juha. (2013). Tietoturvaa toteuttamassa. Tietosanoma. ISBN 978-951-885-334-6.

Andreasson, Kim. (2012). Cybersecurity: Public Threats and Responses. Public Administration and public policy/165. CRC Press. Noudettu 6.12.2023: https://library.oapen.org/bitstream/handle/20.500.12657/40114/9781439846636.pdf?sequence=1&isAllowed=y

Dawes, S. Sharon. (2008). The Evolution and Continuing Challenges of E-Governance. Teoksessa: Public Administration Review, December 2008.

Dworkin, Ronald. (1977, 1978). Taking Rights Seriously. Harvard University Press. Cambridge, Massachusetts.

Halperin, Daniel., Heydt-Benjamin, Thomas S., Ransford, Benjamin., S. Clark, Shane., Defend, Benessa., Morgan, Will., Fu, Kevin., Kohno, Tadayoshi. & H. Maisel, William. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. 2008 IEEE Symposium on Security and Privacy, Oakland, CA, USA.

Heuru, Kauko, 2003, Hyvä hallinto, Edita Oy. ISBN 951-37-3942-2

Hirvonen, Ari: Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Helsinki 2011.

Koivisto, Ida, 2011, Hyvän hallinnon muunnelmat. Väitöskirja, Helsingin yliopisto.

Koivisto, Ida & Koulu, Riikka, 2020, Miten hyvä hallinto digitalisoidaan? Haaste oikeustieteelliselle tutkimukselle, Lakimies 6/2000.

Korhonen, Rauno. (2006). Informaatio-oikeuden asemasta oikeuksien kentässä. Teoksessa: Oikeusteorian poluilla, Professori Rauno Halttusen juhlakirja. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 42. Rovaniemi.

Koulu, Riikka & Sankari, Suvi & Sormunen, Sofia. (2022). Digitalisoituva julkishallinto: käytettävyys kuuluu kaikille. Edilex 2022/36.

Kulla, Heikki & Salminen, Janne. 2021. Hallintomenettelyn perusteet. Alma Talent Oy.

Mäenpää, Olli. (2008). Oikeus hyvään hallintoon. Helsingin yliopiston oikeustieteellinen tiedekunta.

Mäenpää, Olli. (2017). Yleinen hallinto-oikeus. Alma Talent Oy.

Mäenpää, Olli. (2018). Hallinto-oikeus. Alma talent Oy.

Mäenpää, Olli. (2020). Julkisuusperiaate. Alma talent Oy.

Mäenpää, Olli. (2021). Hallintolaki ja hyvän hallinnon takeet. Edita Oy.

Mäenpää, Olli. (2023). Hallinto-oikeus. Alma talent Oy

Nuotio, Kimmo, 2020, Oikeustiede ajassa, teoksessa: Oikeus, Vuosikerta. 49, Nro 4, Sivut 509–519.

Pöysti, Tuomas., Saarenpää, Ahti., Balboa-Alcoreza, Ruxandra., Sarja, Mikko., Still, Viveca. (1997). Tietoturvallisuus ja laki: näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä: tutkimusraportti. Valtiovarainministeriö, Lapin yliopiston oikeusinformatiikan instituutti. ISBN 951-53-1675-8.

Pöysti, Tuomas. (1999). Tehokkuus, informaatio ja eurooppalainen oikeusalue. FORUM IURIS.

Pöysti, Tuomas. (2002). Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet. Teoksessa: Viestintäoikeus. WSOY lakitieto.

Råman, Jari. (2006). Tietoturvallisuus on myös perusoikeus. Teoksessa: Lakimies 5/2006.

Saarenpää, Ahti (1999). Oikeusinformatiikka. Teoksessa: Encyclopaedia Iuridica Fennica 7, Oikeuden yleiset tieteet. Suomalainen Lakimiesyhdistys.

Saarenpää, Ahti. (1999). Informaatio-oikeus. Teoksessa: Encyclopaedia Iuridica Fennica 7, Oikeuden yleiset tieteet. Suomalainen Lakimiesyhdistys.

Saarenpää, Ahti. (2000). Verkkoyhteiskunnan oikeutta – johdatusta aiheeseen.

Saarenpää, Ahti & Wiatrowski, Aleksander. (2016). Society trapped in the network.

Saarenpää, Ahti & Riekkinen, Juhana. (2023). Oikeusinformatiikan perusteet. Lapin Yliopisto. ISBN 978-952-337-347-1

Siltala, Raimo. (2003). Oikeustieteen tieteenteoria. Suomalainen Lakimiesyhdistys.

Szczepaniuk, Edyta Karolina & Szczepaniuk, Hubert & Rokicki, Tomasz & Klepacki, Bogdan. (2020). Information security assessment in public administration. Teoksessa: Computers & Security, Volume 90.

Tolonen, Hannu. (2008). Oikeuden kaleidoskooppi. Suomalaisen lakimiesyhdistyksen julkaisuja E-sarja N:o 19. Helsinki.

Tuori, Kaarlo. Kriittinen oikeuspositivismi. Helsinki 2000.

Turunen, Maija. (2018). Informaatio-oikeuden periaatteet ja tiedonantovelvollisuudet luottolaitosten ja vakuutusyhtiöiden kuluttaja-asiakkaiden luotto- ja vakuutussopimuksissa. Rovaniemi.

Tähti, Aarre. (1995). Periaatteet Suomen hallinto-oikeudessa. Jyväskylä 1995. [väitöskirja].

Tähti, Aarre. (1999). Oikeudellisilla periaatteilla argumentoimisen erityispiirteistä. Lakimies 4/1999.

Voutilainen, Tomi. (2007). Hyvä sähköinen hallinto. 2. painos. Edita Oy.

Voutilainen, Tomi. (2009). ICT-oikeus sähköisessä hallinnossa. [väitöskirja]. Helsinki.

Voutilainen, Tomi. (2012). Oikeus tietoon – informaatio-oikeuden perusteet. Edita Oy.

Voutilainen, Tomi. (2018). Chatbot-sovellus osana viranomaisten neuvontapalveluja. Lakimies 7–8/2018 s. 904–927.

Voutilainen, Tomi. (2019). Oikeus tietoon – informaatio-oikeuden perusteet 2. painos. Edita Oy.

Voutilainen, Tomi. (2023). Digitaalisten palveluiden sääntely. Alma talent Oy.

Wallin, Anna-Riitta & Konstari, Timo. (2000). Julkisuus- ja salassapitolainsäädäntö: laki viranomaisten toiminnan julkisuudesta ja siihen liittyvät lait. Gummerus Kirjapaino Oy