JYU DISSERTATIONS 774

Aapo Immonen

Tapaustutkimus – tiedolla johtaminen kansainvälisten pilvipalveluiden tietosuojatyössä

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 774

Aapo Immonen

Tapaustutkimus – tiedolla johtaminen kansainvälisten pilvipalveluiden tietosuojatyössä

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi Agoran auditoriossa 2
toukokuun 10. päivänä 2024 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 2, on May 10, 2024, at 12 o'clock.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2024

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Päivi Vuorio
Open Science Centre, University of Jyväskylä

ISBN 978-952-86-0128-9 (PDF)
URN:ISBN:978-952-86-0128-9
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-952-86-0128-9

ABSTRACT

Immonen, Aapo
Case study – Managing with information in the data protection work of international cloud services.
Jyväskylä: University of Jyväskylä, 2024, 173 p.
(JYU Dissertations
ISSN 2489-9003; 774)
ISBN 978-952-86-0128-9 (PDF)

This doctoral research is a constructive case study on the perceptions of the different manager levels working in the Finnish government administration, particularly at the Government ICT Centre Valtori regarding data privacy issues.

In recent years, there has been critical discussion in the Finnish public administration about whether the cloud services being used meet the requirements of the EU General Data Protection Regulation (GDPR). Similar discussions have been actively taking place across the European Union member states as well. Based on recent international news coverage, this issue is highly relevant and significant. This debate led to the consideration of the required expertise to achieve privacy by design-based personal data processing when using cloud services, as well as the level of privacy maturity in government administration. This led to the research question: Does the level of data protection competence among different management levels in the target organization, Valtori, meet the requirements of the EU General Data Protection Regulation?

The hypothesis of the study is that experts in different management positions within the target organization can derive meaningful information from the information security domain to support compliant privacy by design work in their professional roles. The study concludes that the hypothesis is not true.

Two separate studies were conducted to answer the research question, spanning from 2019 to 2022. The first study employed a quantitative approach, where representatives from different management levels at Valtori were asked to provide their opinions on statements regarding data privacy. The second study, qualitative in nature, involved interviews with data protection experts working in government administration as well as technical security experts in commercial ICT service production. The aim of combining these different research approaches, known as triangulation, was to achieve a comprehensive and reliable understanding of the phenomenon under examination.

Based on the new knowledge obtained, a constructive operational model for privacy work is developed in the study, which has not been previously presented in the literature. This model supports data protection work concerning cloud services within the framework of information-driven management theory.

Keywords: cloud services, Knowledge Management, Privacy by Design

TIIVISTELMÄ

Immonen, Aapo
Tapaustutkimus – Tiedolla johtaminen kansainvälisten pilvipalveluiden tietosuojatyössä
Jyväskylä: Jyväskylän yliopisto, 2024, 173 s.
(JYU Dissertations
ISSN 2489-9003; 774)
ISBN 978-952-86-0128-9 (PDF)

Tämä väitöstutkimus on luonteeltaan konstruktiivinen tapaustutkimus valtionhallinnossa, erityisesti Valtorissa, työskentelevien johtohenkilöiden käsityksistä tietosuojatyöstä pilvipalveluissa.

Suomen julkishallinnossa on viime vuosien aikana käyty kriittistä keskustelua siitä, täyttävätkö käytössä olevat pilvipalvelut EU:n tietosuoja-asetuksen vaatimukset. Samaa keskustelua käydään aktiivisesti myös laajemmin EU:n alueella. Viimeaikaisen kansainvälisen uutisoinnin perusteella kysymys on laajasti ajankohtainen ja aiheellinen. Keskustelu johdatti pohtimaan, mitä osaamista vaaditaan, jotta pilvipalveluiden käytössä saavutetaan oletusarvoinen ja sisäänrakennettu tietosuoja, ja millainen on valtionhallinnossa tietosuojan kypsyystaso. Tämän perusteella syntyi tutkimuskysymys: Miten kohdeorganisaation, Valtorin, eri johtotasojen tietosuojaosaamisen taso täyttää EU:n tietosuoja-asetuksen vaatimukset?

Tutkimuskysymykseen haettiin vastausta kahdella erillisellä tutkimuksella, jotka toteutettiin vuosina 2019–2022. Ensimmäiseksi tehtiin määrällinen tutkimus, jossa Valtorin eri johtotasojen edustajia pyydettiin ottamaan kantaa tietosuojaa koskeviin väittämiin. Toisessa, laadullisessa tutkimuksessa haastateltiin sekä valtionhallinnossa toimivia tietosuoja-asiantuntijoita että kaupallisessa ICT-palvelutuotannossa työskenteleviä teknisiä tietoturva-asiantuntijoita. Erilaisten tutkimusten yhdistämisen eli triangulaation tavoitteena on saavuttaa laaja-alainen ja luotettava ymmärrys tutkittavasta ilmiöstä.

Tutkimuksen hypoteesina on, että kohdeorganisaation eri johtotehtävissä toimivat asiantuntijat pystyvät muodostamaan tietosuojaa koskevasta informaatiosta ammatillisen roolinsa kannalta merkityksellistä tietoa vaatimustenmukaisen tietosuojatyön toteuttamiseksi. Tutkimuksen mukaan hypoteesi ei kaikilta osin pidä paikkaansa.

Uuden tiedon perusteella tutkimuksessa rakennetaan tietosuojatyön konstruktiivinen toimintamalli, algoritmi, jota ei kirjallisuudessa ole aiemmin esitetty. Se tukee pilvipalveluita koskevaa tietosuojatyötä tiedolla johtamisen teorian viitekehyksestä.

Avainsanat: pilvipalvelut, tiedolla johtaminen, oletusarvoinen ja sisäänrakennettu tietosuoja

Author

Aapo Immonen
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisors

Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Jukka Soininen
TCD Consulting and Research Oy
Finland

Reviewers

Professor Kirsi Helkala
Norwegian Defence Cyber Academy
Norwegian Defence University College
Norway

Principal Lecturer Jyri Rajamäki
Laurea University of Applied Sciences
Finland

Opponent

Principal Lecturer Jarmo Ahonen
Yrittäjyys ja myynti
Tekniikka ja liiketoiminta
Turku University of Applied Sciences
Finland

ESIPUHE

Arvoisa lukija,

On suuri ilo ja kunnia esitellä teille tämä väitöskirjatyö, joka kumpuaa monien vuosien syvällisestä – jopa karikkoisesta – tutkimusmatkasta. Työni pyrkimyksenä on syventää ymmärrystämme ja tietämystämme tietosuojasta pilvipalveluiden käytössä sekä tarjota uusia näkökulmia ja ratkaisuja esiin nouseviin haasteisiin.

Väitöskirjani on saanut alkunsa useiden asiantuntijoiden, tukijoiden ja kollegoiden luotsaamana ja inspiroimana. Haluan ensimmäisenä kiittää ohjaajiani, FT Jukka Soinista, sekä professori Mikko Siposta, joiden johdolla olen saanut kasvaa tutkijana ja laajentaa ymmärrystäni niin tutkimusmenetelmistä kuin tutkittavastakin ilmiöstä. Heidän tuellaan olen oppinut olemaan utelias, kriittinen ja tinkimätön tiedon etsinnässä. Haluan myös kiittää Hannu Rantasta sekä Juha Kinnusta, joiden sytyttämä kipinä kannusti minua aikanaan ryhtymään tutkimustyöhön. Taina Ruottisen ja Anssi Virtasen panos tämän työn viimeistelyssä on ollut korvaamaton; lämpimät kiitokset heille käytetystä ajasta ja taidokkaasta työstä.

Ilman tukea ja kannustusta tämäkään työ ei olisi nähnyt päivänvaloa. Haluan esittää kiitokseni kaikille Valtorin työntekijöille, organisaation ylimmälle johdolle asti. Erityisesti haluan kiittää esihenkilööni, Sonjaa, ja yksikkömme johtajaa, Hannua, heidän ymmärtäväisyydestään ja kärsivällisyydestään. Erityiskiitokset kuuluvat myös Valtorin turvallisuusyksikölle, jonka ainutlaatuinen osaaminen on edesauttanut tämän työn toteuttamista.

Matkan varrella olen kohdannut monia ihmisiä, jotka ovat vaikuttaneet ja mahdollistaneet tämän työn synnyn. Valitettavasti en kykene mainitsemaan heitä kaikkia nimeltä. Haluan kuitenkin kiittää kaikkia, jotka ovat osallistuneet tutkimustyöhöni antamalla arvokasta aikaansa haastatteluihin, kyselyihin tai muilla tavoin jakaneet tietoa kanssani. Ilman tätä vuorovaikutusta tämä työ ei olisi ollut mahdollista.

Lämpimät kiitokset myös ystävilleni ja perheelleni, jotka ovat tukeneet minua vuosien aikana. He ovat olleet minulle suureksi voimavaraksi ja auttaneet minua jaksamaan vaikeina hetkinä. Suvi, Riku ja Nelli, te olette minulle rakkaita. Kiitos Merjalle siitä, että pidit lapsista huolta, kun en ollut paikalla. Pekka, kiitos lukuisista innostavista keskusteluista.

Tämä väitöskirjatyö ei ole pelkkä akateeminen harjoitus, vaan se pyrkii tuomaan uutta tietoa ja ymmärrystä yhteiskuntaamme. Toivon, että työni innoittaa muita tutkijoita jatkamaan tutkimuksen polulla ja antaa eväitä päätöksentekijöille käytännön haasteiden ratkaisemiseen.

Lopuksi haluan kiittää teitä, arvoisat lukijat, jotka olette käyttäneet aikaanne ja kiinnostuneet tutustumaan tähän työhön. Toivon, että löydätte tästä tutkielmasta ajatuksia herättäviä näkökulmia ja uusia oivalluksia. Toivon ja uskon, ettei tutkimusmatkani pääty tähän, vaan aion jatkaa innokkaasti oppimisen ja tiedon jakamisen polulla.

Tämä työ on omistettu niille kahdelle, jotka ovat inspiraationi lähde: isälleni Mikolle ja lapsenlapselleni Jalavalle. On valitettavaa, että heidän tiensä eivät kohdanneet.

Kiitos tästä matkasta. Kohti uutta, sillä maailmassa on vielä paljon hyvää ja kaunista.

Rovaniemellä 1.1.2024
Aapo Immonen

KESKEISIÄ LAKEJA JA ASETUKSIA

Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015). https://www.finlex.fi/fi/laki/ajantasa/2015/20150010

Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013). https://www.finlex.fi/fi/laki/alkup/2013/20131226

Sähköisten viestinnän palvelulaki. Laki sähköisen viestinnän palveluista (917/2014). https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Tiedonhallintalaki. Laki julkisen hallinnon tiedonhallinnasta (906/2019). https://www.finlex.fi/fi/laki/alkup/2019/20190906

Tietosuoja-asetus. EU:n yleinen tietosuoja-asetus (2016/679). https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Tietosuojalaki (1050/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

TORI-laki. Laki valtion yhteisten tieto- ja viestintäteknisten palveluiden järjestämisestä (1226/2013). https://www.finlex.fi/fi/laki/ajantasa/2013/20131226

TUVE-laki. Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015). https://www.finlex.fi/fi/laki/ajantasa/2015/20150010

Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta (1109/2015). https://www.finlex.fi/fi/laki/alkup/2015/20151109

Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (132/2014). https://www.finlex.fi/fi/laki/ajantasa/2014/20140132

Yksityisyyslaki. Laki yksityisyyden suojasta työelämässä (759/2004). https://finlex.fi/fi/laki/ajantasa/2004/20040759

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Euroopan unionin yleisessä tietosuoja-asetuksessa (GDPR) esitetyt tarkat henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat vaatimukset koskevat kaupallisten toimijoiden lisäksi myös viranomaisia. Tietosuoja-asetuksen yksiselitteinen tavoite on niiden ihmisten, joiden henkilötietoja käsitellään, eli rekisteröityjen oikeuksien toteutuminen. Vaatimuksia sovelletaan sekä eurooppalaisiin organisaatioihin, jotka käsittelevät ihmisten henkilötietoja EU:ssa, että EU:n ulkopuolisiin organisaatioihin, jotka käsittelevät EU:n alueella asuvien ihmisten henkilötietoja.

Henkilötietojen käsittely pilvipalveluissa on moniulotteista. Siinä on osattava ottaa huomioon monia osa-alueita, esimerkiksi lainsäädäntö, tekniset ratkaisut ja riskinhallinta. Tämä johtaa työpaikoilla hallitsemattomaan informaatiomyrskyyn, josta tietosuojatyötä vastaavan johdon on miltei mahdotonta seuloa päätöksenteon kannalta merkityksellistä informaatiota. Päätöksenteko vaatii taustalleen tietosuojan hallintamallin, jota hyödyntämällä ilmiötä voi tarkastella sekä kokonaisuutena että osa-alueittain. Päätöksenteon perusvaatimuksena on, että käytettävissä oleva informaatio perustuu näyttöön ja että se on päättäjälle merkityksellistä tietoa (Sund ym. 2004).

Digitalisaatio on yhteiskunnan kehityksessä peruuttamaton ilmiö, ja valtionhallinnon tulee olla tässä kehityksessä edelläkävijä. Tämä tosiasia tekee edellä kuvatun kehityksen haltuunoton välttämättömäksi.

Tietojenkäsittelytieteen historiasta voidaan tunnistaa juurisyitä siihen, miksi henkilötietojen käsittelyyn liittyvien kysymysten haltuun saaminen on haasteellista. Merkittävin syy näyttää olevan se, että pilviteknologian ekosysteemit ovat rakentuneet kauan ennen EU:n tietosuoja-asetuksen voimaanastumista ja esitetyt vaatimukset ovat ristiriidassa pilviekosysteemien ominaisuuksien kanssa. Lisäksi ristiriitaa syntyy tietosuoja-asetuksen ja muun kansallisen tietosuojalainsäädännön kanssa. Globaalit toimijat tasapainoilevat näiden tosiasioiden kanssa ja joutuvat arvioimaan tietosuoja-asetuksen vaatimien muutosten suhdetta vallitsevaan markkinatilanteeseen.

Pilviteknologia avaa mahdollisuuden ennennäkemättömän suurelle henkilötietojen käsittelylle. Organisaatiot ja viranomaiset kasvattavat jatkuvasti

pilviteknologian käyttöä ja sen seurauksena lisäävät samassa suhteessa henkilötietojen keräämistä. Rekisteröityjen näkökulmasta tilanne alkaa näyttää hallitsemattomalta, sillä henkilötietoja käsittelevillä toimijoilla ei ole esittää selkeää näkymää henkilötietovirroista tai dokumentaatiota käsittelyn perusteista rekisteröityjen oikeuksien turvaamiseksi. Tietovirroille ei näy olevan mitään rajaa, ja uutta tietoa muodostetaan yhdistelemällä tietoja eri pisteissä. Tämä tilanne herätti oikeuskomissaarina toimineen Viviane Redingin ajamaan EU:n tietosuoja-asetuksen toteutumista (Danescu 2022).

Tässä työssä tuodaan esiin, millaisia potentiaalisia ristiriitoja globaalien pilvipalveluiden henkilötietojen käsittelyssä on EU:n tietosuoja-asetukseen nähden. Tutkimuksen kohteena olleessa organisaatiossa ja laajemminkin valtionhallinnossa eri päätöksentekoportaiden tulee kyetä reagoimaan tilanteisiin, joissa kansallinen turvallisuus tai taloudellisen hyödyn maksimointi arvotetaan yksityisyydensuojan edelle. Tutkimuksessa käsitellään myös tietosuojatyön epäselviä rooleja, vastuita ja velvoitteita. Euroopan unionin alueen yhteinen tietosuoja-asetus vaatii organisaatioiden johdolta entistä yksityiskohtaisempaa henkilötietojen käsittelyn kokonaisturvallisuuteen liittyvää suunnittelua, johon myös tietosuoja keskeisesti nivoutuu. Tässä tutkimuksessa selvitetään, miten valmis tutkittavan organisaation ja laajemmin valtionhallinnon johto on vastaamaan nykyisiin tietosuojavelvoitteisiin tiedolla johtamisen keinoin.

Väitöskirjatutkimuksen kontribuutiona voidaan pitää työssä esille nouseva näkökohta: Valtorissa ja laajemminkin valtionhallinnossa eri päätöksentekoportaiden tulee kyetä reagoimaan ristiriitoihin, joita syntyy, kun globaalien pilvipalveluiden tarjoajat noudattavat sellaista lainsäädäntöä, joka arvottaa ulkomaalaisen valtion oman ”kansallisen turvallisuuden” (national security) yksityisyydensuojan edelle (Pohjalainen 2018). Myös tietosuojatyön roolit, vastuut ja velvoitteet ovat toimijoille epäselvät. Euroopan unionin alueen yhteinen tietosuoja-asetus vaatii organisaatioiden johdolta entistä yksityiskohtaisempaa tietoturvallisuuteen liittyvää suunnittelua henkilötietojen käsittelyssä.

Uutena tietona syntyi myös ymmärrys siitä, että Valtorissa, ja jopa laajemmin valtionhallinnossa, tietosuojan osaamisen kypsyystaso ei vastaa kaikilta osin tietosuojalle asetettuja vaatimuksia. Tämän perusteella voidaan tehdä johtopäätös, että informaatio ei voi ohjata päätöksentekoa, koska päättäjät eivät saa heille merkityksellistä tietoa ymmärrettävässä muodossa.

Uuden tiedon perusteella tutkimuksessa rakennetaan tietosuojatyön konstruktiivinen toimintamalli, algoritmi, jota ei kirjallisuudessa ole aiemmin esitetty. Se tukee pilvipalveluita koskevaa tietosuojatyötä tiedolla johtamisen teorian viitekehyksestä. Tutkimuksen kohteen tarkastelu sekä työssä syntyneet suuntaviivat tietosuojatyön toiminnan kehittämiselle perustuvat tiedolla johtamisen teorian viitekehykseen (Marr 2010). Tässä kontekstissa ei ole aiemmin tutkittu tiedolla johtamista.

1.1 Tutkimuksen taustaa

Digitalisaatio ja teknologian kehitys tarjoavat organisaatioille aivan uudenlaisen tavan hyödyntää yksityisistä henkilöistä kerättyä tietoa. Henkilötiedoista on muodostunut hyödyke, jota organisaatiot ympäri maailmaa hyödyntävät mitä erilaisimpiin tarkoituksiin. Kulttuurierojen vuoksi tilanne on johtanut jopa myrskyisiin konflikteihin sekä kiivaisiin geopoliittisiin erimielisyyksiin (Dinev 2014).

Organisaatiot ja viranomaiset kasvattavat jatkuvasti informaatioteknologian käyttöä ja sen seurauksena lisäävät samassa suhteessa henkilötietojen keräämistä (Matinmikko 2020, 4). Seurauksena tästä on, että henkilötietojen käyttö muuhun kuin sen alkuperäisen luovutuksen tarkoitukseen on laajentunut siihen pisteeseen, että Euroopan unionin alueella eri tietosuojaviranomaiset ovat ryhtyneet toimenpiteisiin henkilötietojen käsittelyn vaatimuksenmukaisuuden varmistamiseksi. Esimerkiksi henkilötietojen myymisestä on tullut niin merkittävää liiketoimintaa, että useat suuret ja arvostetut yritykset jakavat asiakkaidensa tietoja eri sidosryhmille varsin matalalla kynnyksellä (Reponen 2021).

Huolimatta julkisuudessa esillä olleista mittavista henkilötietojen käsittelyyn liittyvistä loukkauksista kuluttajat eli rekisteröidyt luovuttavat herkästi henkilökohtaisia tietojaan. Julkisuudessa onkin alettu olla enenevässä määrin huolissaan siitä, miten ja missä henkilötietoja käsitellään. Tästä huolimatta rekisteröidyt ovat entistä suostuvaisempia luovuttamaan henkilötietojaan laajamittaisesti uusiin digitaalisiin palveluihin paremman palvelun ja toimivamman yhteiskunnan toivossa. Ilmiötä on alettu osuvasti kutsua yksityisyysparadoksiksi (Taivalmaa 2021, 6).

Yksityisyydellä on yksilöllinen ja yhteiskunnallinen, joskaan ei absoluuttinen arvo. Yhtä yhteisesti omaksuttua yksityisyyden tulkintaa ei ole olemassa eri kulttuureissa tai tieteenaloilla. Tulkintaeroista keskustellaan jatkuvasti, mutta edelleen vallitsee erimielisyyttä siitä, missä määrin yksityisyys-käsite voidaan yleistää. Keskusteleminen pelkästään tietosuojan normeista ja säännöistä tuo vain vähän lisätietoa esimerkiksi siitä, pitäisikö tietosuojaan liittyvää yksityisyyttä pitää oikeutena vai hyödykkeenä. (Richards & Solove 2007.)

Rekisteröidyn eli tavallisen ihmisen näkökulmasta tilanne alkaa näyttää hallitsemattomalta, sillä henkilötietoja käsittelevillä toimijoilla ei ole esittää läpinäkyviä ja selkeitä perusteluja henkilötietojen käsittelylle eikä näkymää henkilötietovirroista, saati dokumentaatiota käsittelyn perusteista rekisteröityjen oikeuksien turvaamiseksi.

Rekisteröidyt eli henkilöt, joiden tietoja käsitellään, ovat alkaneet olla yhä enenevässä määrin huolissaan siitä, miten ja missä heidän henkilötietojaan käsitellään. Tästä huolimatta he luovuttavat edelleen henkilötietojaan.

EU:n alueella ilmiötä on alettu tarkastella kansalaisten, siis rekisteröityjen, keskeisen perusoikeuden eli yksityisyyden suojan näkökulmasta (Syrjänen 2006, 61). Vuonna 2016 voimaan astunut ja toukokuusta 2018 alkaen sovellettu EU:n yleinen tietosuoja-asetus (GDPR, General Data Protection Regulation) sekä vuonna 2018 voimaan astunut kansallinen tietosuojalainsäädäntö ovat luoneet

organisaatioiden henkilötietojen käsittelyn toimintatapoihin muutostarpeen, jonka vaikutus on tunnistettu Suomessa myös julkishallinnossa. EU:n tietosuoja-asetus tuli sovellettavaksi sellaisenaan kaikkiin EU-maihin, ja se synnytti uuden ja merkityksellisen prosessinmuutoksen kaikessa henkilötietojen käsittelyssä. (Tietosuoja-asetus 2016/679.) EU:n tietosuoja-asetuksen keskeinen ydinajatus on se, että yksittäinen kansalainen saa aiempaa vahvemman itsemääräämisoikeuden ja kontrollin omiin yksilöiviin henkilötietoihinsa suhteessa globaaleihin toimijoihin.

Yhdysvaltalaiset toimijat dominoivat pilvipalveluiden teknologiamarkkinoita, ja siksi henkilötietoja siirtyy Yhdysvaltoihin valtavalla volyymilla. Tietosuoja oletusarvona ja sisäänrakennettuna tietojenkäsittelyyn, uudet vakiosopimusehdot sekä ennakoiva riskiarviointityö ovat komission vastaus henkilötietojen siirtoihin kohdistuviin epäselvyyksiin, jotka koskevat erityisesti viranomaisten pääsyä dataan, tehokkaiden oikeussuojakeinojen puuttumista sekä sitä, ettei rekisteröityjen tietosuojaoikeuksien toteutumista voida taata. Huomionarvoista on, että Yhdysvaltojen tiedustelulait ulottavat lonkeronsa myös yhdysvaltalaisten yhtiöiden eurooppalaisiin tytäryhtiöihin, vaikka ne sijaitsevat Euroopassa. (Rautiainen 2021.)

EU:n tietosuoja-asetuksen voimaanastumisen jälkeen viranomaiset ovat joutuneet entistä tarkemmin riskiperusteisesti arvioimaan rekisteröityjen oikeuksien toteutumista myös pilvipalveluissa. Tämä pitää sisällään sekä laaja-alaista riskinarviointia että tietosuojan ja tietoturvan uudelleenarviointia tietojärjestelmätieteen viitekehyksestä. Tämän lisäksi pilvipalvelutoimittajien monimutkaisten sopimuskokonaisuuksia suhteessa EU:n tietosuoja-asetuksen ja kansallisen lainsäädännön arvioimista juridisesta viitekehyksestä tulee tarkentaa. Edellä kuvattujen kokonaisuuksien tarkastelu on jo johtanut rakenteellisiin ja toiminnallisiin muutoksiin henkilötietojen käsittelyssä pilvipalveluissa.

Esimerkiksi Facebookin oikeuksia henkilötietojen käsittelyssä on jouduttu tarkastelemaan uudelleen. Itävaltalaisaktivisti Max Schrems teki nimittäin Irlannin tietosuojavaltuutetulle valituksen Facebookissa tapahtuvasta henkilötietojen käsittelystä. Schrems esitti perustelut, joilla Facebookia voidaan kieltää siirtämästä tietoja Irlannista Yhdysvaltoihin. Hän väitti perustellusti Facebookin osallistuvan yhdysvaltalaisviranomaisten joukkovalvontaohjelmaan, joka tunnetaan Foreign Intelligence Surveillance Act (FISA) -lakina. Schrems perusti valituksensa EU:n tietosuojalainsäädäntöön, joka ei salli tiedonsiirtoa EU:n ulkopuolisiin maihin, ellei yritys pysty takaamaan riittävää suojaa. Syyskuussa 2020 Irlannin tietosuojakomissio lähetti Facebookille alustavan määräyksen lopettaa EU:n kansalaisten tietojen siirtäminen Yhdysvaltoihin (Aktipis & Katwan 2021, 53–98). Pilviteknologian käytön kannalta muutokset ovat olleet pakollisia, ja toimijoiden rooleja, vastuita ja velvoitteita on ollut uudelleenarvioitava yhteisen ymmärryksen aikaansaamiseksi.

Tietojärjestelmätiede pitää sisällään tietojärjestelmien suunnittelua, rakentamista ja toimintaa sekä sovellusten ja järjestelmien käyttöä, johon myös ihmiset, organisaatiot ja yhteiskunta yhdistyvät (Soininen 2021, 7). Tietojärjestelmätieteellä on globaalissa kehityksessä keskeinen rooli, koska sen fokuksessa on tieto-

ja viestintätekniikan mahdollisimman tehokas käyttö, jolla edistetään mm. organisaation tuloksellisuutta. Julkissektorilta ei odoteta voittoa kuten yksityissektorin toimijoilta, jolloin tuloksellisuutta voidaan tulkita kansalaisten oikeudeksi saada hyviä ja lainmukaisia palveluja vastineeksi verorahoilleen. (Lumijärvi 2015, 75; Sinervo ym. 2015, 97.)

Tietoturva on keskeinen tietojärjestelmätieteitä läpileikkaava funktio. Koska perusvaatimuksena on, että henkilötietojen käsittely tapahtuu vaatimusten mukaisissa ympäristöissä, sitovat edellä kuvatut ominaisuudet tietosuojan kiinteäksi osaksi tietojärjestelmätieteitä. Tietosuoja on rekisteröidyn oikeus, jonka laki takaa kaikille yksilöille. Tietosuojan keskiössä ovat rekisteröidyt, rekisterinpitäjät sekä niiden lukuun toimivat tietojenkäsittelijät, joiden toimintaan EU:n tietosuoja-asetuksella ja kansallisilla tietosuojalaeilla vaikutetaan (Kataja 2021).

Henkilötietojen käsittelyä ohjattiin Suomessa aiemmin henkilötietolailla, joka sittemmin kumottiin EU:n tietosuoja-asetuksen voimaan astumisen myötä. Lisäksi henkilötietojen käsittelyä ohjaa moni kansallinen lainsäädäntö. Tietosuoja-asetuksen mukanaan tuoma uudistus koskee tutkimuksen kohteena olevan organisaation, Valtion tieto- ja viestintätekniikkakeskuksen Valtorin, lisäksi myös koko julkista sektoria. Tietosuoja-asetuksen voimaanastumisen myötä valtionhallinto kokonaisuudessaan joutuu tarkastelemaan rekisteröityjen oikeuksien, vapauksien sekä yksityisyydensuojan toteutumista tietojenkäsittely-ympäristöissä aivan uudesta näkökulmasta, mikä tuo mukanaan uusia haasteita, mutta oikein implementoituna tuottaa kilpailuetua sen periaatteita kunnioittaville toimijoille.

Henkilökohtaiset kokemukseni tietosuojavastaavan tehtävistä ja niihin kohdistuneista haasteista herättivät lopullisen päätöksen tutkimukseni aiheen valinnassa. Huomioni kiinnittyi erityisesti siihen, että johdon ohjeistamat konkreettiset toimenpiteet, joilla asetuksen vaatimuksia on tarkoitus noudattaa julkishallinnon eri organisaatioissa, ovat olleet varsin kirjavia ja jopa ristiriidassa sekä tietosuoja-asetuksen että toisten toimijoiden tietosuojatyön kanssa. Tulkintani on, että suurimmat esteet edellä mainittujen toimenpiteiden toteutumiselle ovat organisaatioiden siiloutuminen sekä tiedon pihtaamisen kulttuuri. Edellä mainitut seikat motivoivat pohtimaan, miten julkishallinnossa toimivan organisaation johdon eri tasot hyödyntävät tietosuojatyössä syntyvää dataa informaation ja tiedon lähteenä johtamisessa ja mikä informaatio on relevanttia johdon eri tasoille, kun organisaation tietosuojaa rakennetaan tietosuoja-asetuksen vaatimusten mukaisesti. Näistä pohdinnoista muodostui työni tutkimuskysymys.

Tutkimus kannustaa jatkamaan jo alkanutta vilkasta keskustelua siitä, miten eri toimijoiden verifioimat lainsäädännölliset, riskinhallinnolliset sekä tietoturvan viitekehykset tulisi harmonisoida, jotta tietosuoja-asetuksen vaatimukset tulisivat kauttaaltaan huomioiduiksi henkilötietojen käsittelyssä Suomen valtionhallinnossa. Tällöin on välttämätöntä ymmärtää kansainvälisten toimijoiden kulttuurisidonnaiset erot pilvipalveluiden käyttöön liittyvän tiedon arvottamisessa, käsittelyssä sekä suojaamisessa.

1.2 Teknologian nopean kehityksen tuomat haasteet

Pilviteknologian kehitys on ollut nopeaa, ja toimittajat ovat tehneet teknologian mukanaan tuomista hyödyistä suuria lupauksia. Kiireisessä kehitystyössä tietosuojalle asetettuja vaatimuksia on joskus sivuutettu. Tällaisista tietosuojarikkomuksista on annettu suuria sanktioita; vuoteen 2019 mennessä suurimpia sanktioita ovat saaneet British Airways, 204 miljoonaa euroa, Mariot Hotel, 110 miljoonaa euroa, ja Google, 50 miljoonaa euroa. Tämän jälkeenkin sanktioita, jopa edellisiä suurempia, on langetettu useita. (Zhao ym. 2023.)

Valtiovarainministeriö on vuonna 2023 linjannut julkishallinnon pilvisiirtymän strategiaksi, että pilvipalveluiden ja pilvipalveluteknologian tulee olla ensisijainen valinta, mikäli estäviä perusteita (teknologiseen) valintaan ei ole. Linjauksen tavoitteena on varmistaa, että uudet tuotteistetut tietoturvallisemmat palvelut ja kyvykkyydet ovat helposti saatavilla sekä käyttöön otettavissa. Palveluiden tulee mahdollistaa joustava käyttö ja kapasiteetin hankinta. (Valtiovarainministeriö 2023.) Valtiovarainministeriön Cirrus-hankkeen yhteydessä julkaistussa Julkisen sektorin pilvipotentiaali Suomessa -hankkeen raportissa, joka esiteltiin huhtikuussa 2023, todetaan, että julkishallinnossa pilvisiirtymän isoin kysymys liittyy tietosuojan haasteisiin (Suonio 2023).

Suomessa tietosuojan viranomaisvastuu on tietosuojavaltuutetun toimistolla, jossa nähdään, että oikein toteutettuna tietosuojatyö vaikuttaa yleiseen kilpailukykyyn positiivisesti. Tietosuojavaltuutetun toimiston strategiassa korostetaan ennakoinnin ja priorisoinnin, osaamisen, informaatio-ohjauksen sekä liittoutumisen merkitystä (Tietosuojavaltuutetun toimisto 2017). Tietosuojan keskeiset periaatteet kiteytyvät oletusarvoisen ja sisäänrakennetun tietosuojan käsitteeseen, jossa edellytetään asianmukaisten teknisten ja organisatoristen toimenpiteiden toteuttamista säädettyjen vaatimusten täyttämiseksi (Tietosuoja-asetus 2016/679, artikla 25, kappale 76).

Organisaatioiden ylimmän tason johtajat ovat reagoineet usealla eri tavalla siihen faktaan, että henkilötietojen asianmukainen käsittely on lopulta heidän vastuullaan. Suomessa julkishallinnossa toimivien organisaatioiden ylin johto pyrkii noudattamaan EU:n tietosuoja-asetusta (2016/679) sekä kansallisen tietosuojalain (1050/2018) vaatimuksia, niin että rekisteröityjen oikeudet toteutuvat.

Suomen julkishallinnossa rekisterinpitäjien teettämissä vaikutusten arvioinneissa (DPIA) on noussut esille useita yksityiskohtia, jotka herättävät kysymyksiä henkilötietojen käsittelyn vaatimuksenmukaisuudesta ja osoittavat jopa merkittäviä epäkohtia rekisteröidyn oikeuksien toteutumisessa. Tiedonsiirtoja koskevien riskinarviointien (TIA) perusteella on todennettu, ettei edes komission lisätoimenpidelinjauksilla ole mahdollista täydentää tietosuojaa siten, että puutteet kolmansien maiden tietosuojan tasossa tulisivat tehokkaasti korjatuiksi.

Kun henkilötietoja siirretään ns. kolmansiin maihin eli EU- ja ETA-alueiden ulkopuolelle, on tehtävä tiedonsiirtoja koskeva riskinarviointi (Transfer Impact Assessment, TIA). Tavoitteena on varmistaa, että sillä maantieteellisellä alueella, jossa EU-kansalaisen henkilötietoja käsitellään, on lainsäädäntö tietosuojan

osalta samalla tasolla kuin EU:n tietosuoja-asetuksessa kuvataan. Henkilötietojen siirroilla kolmansiin maihin tarkoitetaan kaikkea henkilötietojen käsittelyä, jossa tieto päätyy Euroopan talousalueen ulkopuolella sijaitsevan toimijan saataville. Rekisterinpitäjä on kokonaisvaltaisesti vastuussa tästä ja myös käsittelijöiden tekemistä tietojensiirroista. Siirtämiseksi katsotaan henkilötietojen tallentaminen ETA-alueen ulkopuolella sijaitsevalle palvelimelle (data in rest) ja teknisen pääsy-yhteyden avaaminen tietoihin ETA-alueen ulkopuolisesta maasta (data in transfer). Lisäksi tarvittaessa vaaditaan lisäsuojakeinoja, jotka täydentävät vakiolausekkeita (standard contractual clauses, SCC). (Sandfuchs 2021, 245–249; Johansson 2022.)

Nämä esille nousseet haasteet tuovat merkittäviä uhkia rekisteröityjen oikeuksille ja vapauksille. Kysymys on EU:n tietosuoja-asetuksen voimaan astumisen myötä ajankohtainen koko EU-alueella, ja sillä on merkittävä vaikutus myös globaalien pilvipalveluiden toimintaan. Haaste on noussut esille useilla eri foorumeilla laajasti EU-alueella. (Aden 2020).

Euroopan tietosuojaneuvosto teki vuonna 2022 EU alueelle laajan tietosuojaan liittyvän kartoituksen, jonka mukaan kaikissa EU:n jäsenmaissa on tunnistettu identtisiä haasteita siinä, miten henkilötietoja käsitellään pilvipalveluissa (EDPB 2020). Haasteet konkretisoituivat heinäkuussa 2020 komission tuomioistuimen päätökseen kumota EU:n ja Yhdysvaltojen välinen Privacy Shield -järjestely, joka oli yksi lainsäädännön mahdollistamista tavoista siirtää henkilötietoja EU:sta Yhdysvaltoihin. Tuomioistuin totesi, että aiempi päätös Privacy Shield -järjestelyn tietosuojan tason riittävyydestä on pätemätön, koska henkilötietoja Yhdysvaltoihin siirrettäessä perusoikeuksiin puuttumista ei ollut rajattu tavalla, joka olisi vastannut EU:n vaatimuksia. Tilanteen kestämättömyyttä kuvaa se tosiasia, että järjestelyn kumoutuminen astui välittömästi voimaan ilman siirtymäaikaa. (Euroopan unionin tuomioistuin 2020.)

Kun tietosuoja-asetusta tarkastellaan jäsenmaiden kompromissina, tietosuojalle asetettujen normien noudattaminen saa korostetun merkityksen. Asetuksessa vaatimukset on kuvattu abstraktilla tasolla, ja jäsenvaltioille on jätetty kansallista liikkumavaraa käytännön toteutuksissa. Tämä taas antaa mahdollisuuden siihen, että tietosuojatyössä käytetään jopa ristiriitaisia toimintamalleja. Nykyistä yhteneväisemmän näkymän tietosuojatyöhön tarjoavat tiedolla johtamisessa kuvatut metodit, kuten tiedon jakaminen sekä SECI-malli.

Tietosuoja itsessään ei tarjoa suoraan teknisiä menetelmiä tai välineitä eitoivottujen henkilötietojen käsittelyyn kohdistuvien poikkeamien haltuun saamiseksi, vaan tietosuojatyössä turvaudutaan hallinnollisiin, fyysisiin ja teknisiin tietoturvakontrolleihin. Tietosuojavaatimuksia implementoitaessa viitataan tietoturvakontrolleihin, joita kuvataan mm. ISO/IEC 17799 -standardissa ja sen myöhemmissä versiossa (Siponen & Willison 2009; Siponen & Baskerville 2018). Jotta tietosuoja ja tietoturva toimivat kiinteästi vuorovaikutuksessa poikkeamatilanteissa, on ymmärrettävä myös, miten poikkeamia koskeva tieto saavuttaa johdon, miten johdolle tuotetaan näistä raportteja sekä ymmärrettävää tietoa ja miten se esitetään ymmärrettävänä tietona päätösten tueksi. Lisäksi on kysyttävä, onko tieto relevanttia johdon näkökulmasta, mihin toimenpiteisiin se johtaa

ja onko toimintamallit kuvattu johtamisen näkökulmasta niin, että ne tukevat sisäänrakennettua ja oletusarvoista tietosuojaa.

Nykyisessä tietosuoja- ja tietoturvatyössä poikkeamiin reagoidaan uhan konkretisoitumisen jälkeen. Tyypillisesti viranomaiset, usein asiantuntijoiden eksplisiittisen tiedon sekä kokemusten kautta syntyneen hiljaisen tiedon avustuksella, pyrkivät saamaan poikkeavan tilanteen haltuunsa hyödyntämällä tilanteissa syntyvää fragmentoitunutta dataa uhan ollessa jo konkretisoitunut, mikä johtaa valitettavan usein monimutkaisten ja toisiinsa vaikuttavien tapahtumasarjojen osaoptimointiin. Poikkeaman uhasta syntyy eri lähteistä huomattava määrä dataa, jota tilanteen haltuun saamiseksi ei organisaatioiden strategisessa johtamisessa näytetä hallittavan. Ei-toivotut poikkeamat saattavat pitkään jatkuessaan muodostaa organisaatiossa kriisin. Kriisinhallintateorioiden mukaan vaikuttavinta kriisinhallintaa on niiden ennaltaehkäisy (Immonen & Rantanen 2011).

Ongelman ytimessä näyttää olevan tiedon muodostuminen ja jakaminen. Ongelma konkretisoituu siten, etteivät eri toimijat saa vastuidensa kannalta merkityksellistä informaatiota päätöksentekonsa tueksi, minkä vuoksi tietosuojan kypsyystaso ei vastaa tietosuoja-asetuksen vaatimuksiin. Tämä johtaa siihen, ettei itse tietosuojatyö voi olla vaatimustenmukaista. Tiedon jakamisella tavoitellaan osaamisen (tietojen ja taitojen) jakamista holistisesti ongelmien ratkaisemista varten.

1.3 Työn tavoitteet, rajaus, tutkimuskysymys ja hypoteesi

Tämä työ koskee **valtionhallinnon oletusarvoista ja sisäänrakennettua tietosuojatyötä käytettäessä kansainvälisiä pilvipalveluita**. Työn tavoitteena on tuottaa näyttöön perustuvaa tietoa siitä, mitä informaatiota kohdeorganisaation eri johtotasot tarvitsevat tietosuojatyön johtamiseen ja päätöksentekoon.

Työn tavoitteiden saavuttamiseksi tutkimus jaettiin kahteen osaan, jotka täydentävät toisiaan. Ensimmäinen tutkimus on määrällinen, ja se kohdennettiin tutkittavana olevan valtionhallinnon organisaation Valtorin eri johtotasoille. Tietoja kerättiin strukturoidulla kyselylomakkeella, jonka väittämät muodostuivat sekä EU:n tietosuoja-asetuksesta että kansallisesta tietosuojalainsäädännöstä. Tulosten perusteella arvioitiin, tunnistavatko eri johtotasot, millaista informaatiota he tarvitsevat tietosuojatiedon muodostamiseksi sekä mikä on kohderyhmän tietosuojaosaamisen kypsyystaso. Toinen tutkimus toteutettiin laadullisena, ja siinä haastateltiin sekä valtionhallinnossa toimivia tietosuoja-asiantuntijoita että kaupallisessa ICT-palvelutuotannossa työskenteleviä teknisiä tietoturva-asiantuntijoita. Tutkimusten tulosten ja näkökulmien yhdistämisen eli triangulaation tavoitteena on saada laaja-alainen ja luotettava ymmärrys tietosuojaosaamisen tasosta. Menetelmien tarkemmat kuvaukset on esitetty luvussa 5.

Kiinnostuksen kohteena on selventää tietosuojan hallintamallia hyödyntämällä, miten Valtorin eri johtotasojen tietosuojaosaamisen taso täyttävät EU:n tietosuoja-asetuksen vaatimukset. Vastausten perusteella voidaan arvioida, mikä

informaatio on relevanttia johtamisessa sekä miten systemaattista näyttöön perustuvan uuden tiedon hyödyntäminen tietosuojatyössä on. Tavoitteena on purkaa Valtorin sisäisiä siiloja, jotta syntynyttä uutta tietoa voidaan jakaa sisäänrakennetun ja oletusarvoisen tietosuojan vaatimusten mukaisesti. Kiinnostuksen kohteena on selventää tietosuojan hallintamallia hyödyntämällä, miten voidaan arvioida, mikä tietosuojatyötä koskeva informaatio on relevanttia johtamisessa sekä miten systemaattista näyttöön perustuvan uuden tiedon hyödyntäminen tietosuojatyössä on, jotta organisaation sisäisiä siiloja voidaan purkaa ja syntynyttä uutta tietoa voidaan jakaa sisäänrakennetun ja oletusarvoisen tietosuojan vaatimusten mukaisesti. Mielenkiinto kohdistuu myös siihen, miten tietojärjestelmätieteen eri osa-alueet – ensisijaisesti tietojärjestelmien toiminta sekä sovellusten ja järjestelmien käyttö, johon ihmiset, organisaatiot ja yhteiskunta keskeisesti kuuluvat – nivoutuvat tietosuojavaatimuksiin.

EU:n tietosuoja-asetuksen lisäksi on siis syytä huomioida tietosuojaa koskevia kansallisia lakeja, henkilötietojen suojaamiseen kohdennettuja tietoturvakontrolleja, Euroopan tietosuojaneuvoston linjauksia ja kansallisen tietosuojaviraston antamia ohjeita. Koska tutkimuksessa mukana olevat pilvipalvelutoimittajat ovat globaaleja toimijoita, ne noudattavat lähtökohtaisesti globaalia lainsäädäntöä, toisin kun EU:n jäsenvaltiot, jotka noudattavat ensisijaisesti EU:n tietosuoja-asetusta. On ollut perusteltua laajentaa tutkimusta koskemaan paitsi EU:n tietosuoja-asetusta myös Yhdysvalloissa sovellettavaa henkilötietojen käsittelyyn liittyvää tietosuojalainsäädäntöä.

Muun muassa Yhdysvalloissa kansallisen turvallisuuden vaatimukset arvotetaan yksityisyyden suojan edelle (Pohjalainen 2018). Koska EU:n alueella toimivat pilvipalveluiden toimittajat ovat käytännössä yhdysvaltalaisia, on tässä tutkimuksessa perusteltua pohtia nimenomaan Yhdysvaltojen lainsäädännön ja EU:n tietosuoja-asetuksen välisen suhteen vaikutuksia tarvittavaan informaatioon tehtäessä rekisteröityjen oikeuksiin liittyviä päätöksiä. Globaalista markkina-asemastaan huolimatta esimerkiksi kiinalainen pilvipalvelun toimittaja Alibaba Cloud sekä venäläinen RuNet rajataan tämän tutkimuksen ulkopuolelle, sillä niiden päämarkkina-alueet ovat Aasia ja Venäjä. (Helin 2021; Talja 2015; Mi ym. 2011.)

Työssä selvennetään, miten kohdeorganisaation johto tietosuojatyössä arvioi poikkeamien aiheuttamien uhkien todennäköisyyttä pilvipalveluissa. Koska riskien vähentämisen eli mitigoimisen ja poikkeamien hallinnan keskeinen keino ovat tietoturvakontrollit, niitä ei voida sivuuttaa tässä tutkimuksessa. Haasteisiin haetaan ratkaisuja tietojärjestelmätieteiden ja tiedolla johtamisen avulla. Kaiken kaikkiaan tietosuojaa tarkastellaan siis riskiperusteisesti juridisesta, hallinnollisesta, operatiivisesta, fyysisestä, teknisestä sekä toiminnallisesta viitekehyksestä.

Päämääränä on konstruoida tiedolla johtamiseen perustuva malli, algoritmi, jolla pragmatisoidaan, miten julkishallinnon strategisessa johtamisessa voidaan hyödyntää tietosuojatyössä syntyvää dataa tai siitä jalostunutta informaatiota oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamiseksi. Aiemmin esitellyistä tavoitteista nousevat luontevasti kysymykset, joiden kautta selvitetään, mikä on toimijoiden ja toimintaympäristön kypsyys toteuttaa vaadittu

muutos oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamiseksi julkishallinnossa EU:n tietosuoja-asetuksen vaatimusten mukaisesti.

Tutkimuskysymykseksi muodostui seuraava:

- Miten kohdeorganisaation eri johtotasojen tietosuojan osaamistaso täyttää EU:n tietosuoja-asetuksen vaatimukset?

Tosiasia on, että valtionhallinnossa päätöksentekijöillä on käytettävissään riittävästi tietoa tietosuojaan liittyvään päätöksentekoon oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamiseksi ja että he voivat sen pohjalta varmistaa oletusarvoisen ja sisäänrakennetun tietosuojan toteutumisen pilvipalveluissa.

Työn hypoteesi on, että kohdeorganisaatiossa eri johtotehtävissä toimivat asiantuntijat pystyvät muodostamaan tarjolla olevan informaation perusteella heidän ammattiroolinsa kannalta merkityksellistä tietoa vaatimustenmukaisen tietosuojatyön toteuttamiseksi.

Hypoteesin pohjalta halutaan selventää, mikä tietosuojatyöstä muodostuva informaatio on relevanttia johtamisen eri tasojen näkökulmista sekä miten systemaattista näyttöön perustuvan uuden tiedon hyödyntäminen tietosuojatyössä on, jotta organisaation sisäisiä siiloja voidaan purkaa ja syntynyttä uutta tietoa voidaan jakaa sisäänrakennetun ja oletusarvoisen tietosuojavaatimusten mukaisesti. Tietosuojan viitekehyksestä operationalisoimalla tiedolla johtamisen teoriaa sekä tunnistamalla tietosuojatyössä esiintyviä heikkoja signaaleja ja varhaisia varoituksia poikkeamatilanteissa mahdollistetaan interventiot mahdollisimman varhaisessa vaiheessa.

Työn tuloksena syntyy näyttöön perustuvaa tietoa tiedolla johtamisen menetelmistä, joita voidaan käyttää kohdeorganisaation eri johtotasoille sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamiseksi. Työssä haetaan monitieteisiä ratkaisuja olemassa oleviin haasteisiin sekä pyritään havainnollistamaan oletusarvoista ja sisäänrakennettua tietosuojaa siten, että aiemmin kuvatut tavoitteet saavutetaan.

Tässä luvussa kuvataan tutkimuksen taustaa (alaluku 1.1), käsitellään pilviteknologian nopean kehityksen tuomia haasteita (alaluku 1.2), kuvataan työn tavoitteet, rajaus, tutkimuskysymys sekä hypoteesi (alaluku 1.3) ja kuvataan Valtoria organisaationa (alaluku 1.4).

Luvussa 2 paneudutaan tietosuojaan ja tietoturvaan: niiden eroihin, kytköksiin, käsitteisiin, tavoitteisiin ja keinoihin. Alaluvussa 2.5 esiteltävä tietosuojan hallintamalli on tutkimuksen keskeinen pohja, sillä tietoturvatyön laajaa kenttää hahmotetaan sen mukaisesti.

Luvussa 3 käydään läpi aiempia tutkimuksia aiheesta. Luvussa 4 esitellään tutkimuksen läpileikkaavia teemoja, jotka käsittelevät pilvipalveluita ja EU:n tietosuoja-asetuksen suhdetta pilvipalveluihin sekä rekisteröidyn oikeuksien toteutumiseen liittyviä vastuukysymyksiä. Lisäksi kappaleessa käydään läpi tiedolla johtamista sekä miten kriisinhallinnan menetelmät voivat tukea tietosuojatyötä.

Luvussa 5 kuvataan tutkimusotetta ja menetelmiä. Luvussa 6 esitellään väitöskirjan kaksi osatutkimusta, ensinnäkin Valtorin eri johtoportaille suunnattu kyselytutkimus ja sitten valtionhallinnon tietoturva-asiantuntijoille tehdyt haastattelututkimukset. Luvun lopuksi kuvataan tutkimusten tuloksia, ja näitä

vedetään yhteen sekä Valtorin kannalta, että aineistosta nousevien teemojen kannalta luvussa 7.

Luku 8 avaa tutkimuksen tulosten merkitystä tulevaisuuden kannalta. Miten organisaatiot voivat hyödyntää tämän tutkimuksen tuloksia? Alaluvussa 8.2.1 esitellään tutkimuksen pohjalta laadittu algoritmi eli malli, jolla organisaatiot voivat selvittää palveluidensa tietosuojan tilannetta ja suunnitella sen kehittämistä jäsennellysti osa-alueittain ja kokonaisuutena. Alaluvussa 8.2.2 nostetaan esiin tutkimushavainnoista megatrendin omaisia aiheita, joihin joko organisaatiot tai koko maailma joutuvat lähitulevaisuudessa ottamaan kantaa ja jotka ohjaavat jatkossa pilvipalveluiden toimivuutta ja turvallisuutta. Lopuksi luvussa 9 on katsaus tutkimuksen luotettavuudesta ja jatkotutkimustarpeista.

1.4 Valtori tutkimuskohteena

Tutkimuksen kohdeorganisaatio on Valtion tieto- ja viestintätekniikkakeskus Valtori. Sen lakisääteisenä tehtävänä on tuottaa valtionhallinnolle toimialasta riippumattomia ICT-palveluita sekä korkean varautumisen ja turvallisuuden vaatimukset täyttäviä tieto- ja viestintäteknisiä palveluja. Näiden tehtävien vuoksi Valtorissa käsitellään poikkeuksellisen paljon yksilöivää henkilötietoa.

Valtorilla on tietosuojan näkökulmasta toistaiseksi kaksi roolia: toimia rekisterinpitäjänä omien tietojensa osalta sekä toimia tietojenkäsittelijänä asiakkaidensa lukuun. Tietosuoja-asetuksen mukaan rekisterinpitäjä määrittelee käsittelyn tarkoitukset ja keinot. Viranomaistoiminnassa viranomaisen ydintehtäviin liittyvästä henkilötietojen käsittelystä määrätään yleensä lainsäädännössä, ja siellä on määritelty tarkoitukset, joihin henkilötietoja käsitellään. Valtorin kohdalla lainsäädäntö (TORI-laki eli laki valtion yhteisten tieto- ja viestintäteknisten palveluiden järjestämisestä 1226/2013 ja TUVE-laki eli laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015) ei kuitenkaan ota kantaa henkilötietojen käsittelyyn. Tämän takia Valtori on katsonut, ettei se pysty ottamaan vastuuta henkilötietojen käsittelyn tarkoituksista muiden viranomaisten puolesta, vaan se toimii pääsääntöisesti henkilötietojen käsittelijänä.

Valtorin asiakaskunta on laaja – siihen kuuluvat kaikki valtionhallinnon virastot ja laitokset –, ja siksi lakisääteinen tehtävä asettaa organisaatiolle poikkeuksellisen korkeat vaatimukset sekä tietosuoja-asetuksen että tietosuojalain noudattamisessa. Valtori on myös asettanut tavoitteekseen olla tietosuojatyön edelläkävijä valtionhallinnossa.

Valtorin perustietotekniikkapalvelutuotanto perustuu lakiin (1226/2013) ja asetukseen (132/2014) valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä sekä lakiin (10/2015) ja asetukseen (1109/2015) julkisen hallinnon turvallisuusverkkotoiminnasta.

Valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämistä koskevan lain mukaisesti Valtorin strategisesta ja liiketoiminnallisten periaatteiden ohjauksesta, toimintalinjoista ja tulostavoitteista vastaa valtiovarainministeriö. Samat periaatteet koskevat valtiovarainministeriön ohjaamaa ja valvomaa, Valtorin

ylläpitämää, korkean varautumisen ja turvallisuuden vaatimukset täyttävää hallinnon TUVE-turvallisuusverkkoa. Tähän viranomaisverkkoon kuuluvat viestintäverkko, siihen liittyvät laitetilat ja laitteet sekä yhteiset tieto- ja viestintätekniset palvelut. Turvallisuusverkolla mahdollistetaan korkeaa varautumista ja turvallisuutta vaativa työskentely.

Julkisen hallinnon turvallisuusverkkotoiminnalla ja toiminnasta annetulla lailla (10/2015) turvataan valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten yhteistyötä ja viestintää kaikissa tilanteissa. Turvallisuusverkon palvelutuotannon ohjauksesta ja valvonnasta vastaa valtiovarainministeriö kuultuaan TUVE-neuvottelukuntaa. TUVE-verkon palveluja käytetään valtioneuvostossa, Poliisihallituksessa, Rajavartiolaitoksessa, Hätäkeskuslaitoksessa, Maahanmuuttovirastossa, Puolustusvoimissa, Tullissa, pelastustoimessa, ensihoidossa sekä muissa viranomaisia tukevissa organisaatioissa.

Julkisen hallinnon turvallisuusverkkotoiminnalla ja toiminnasta annetulla lailla (10/2015) turvataan valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten yhteistyötä ja viestintää kaikissa tilanteissa. Turvallisuusverkon palvelutuotannon ohjauksesta ja valvonnasta vastaa valtiovarainministeriö kuultuaan TUVE-neuvottelukuntaa.

2 TIETOSUOJA JA TIETOTURVA

Teknologian kehitys on johtanut siihen, että tietojenkäsittely-ympäristö on muuttunut entistä monimutkaisemmaksi. Digitalisaatio, globalisaatio, teknologian nopea kehitys sekä kansalaisten ja viranomaisten virastoille asettamat korkeat laatuvaatimukset henkilötietojen käsittelylle luovat valtionhallinnon eri toimijoille paineita toimia teknologian kehityksen aallonharjalla. Digitaalisuuden vaikutus on väistämättä muuttanut toimialojen luonnetta, ja trendi kiihtyy tulevaisuudessa. Samalla sekä kansalaisten (tietosuoja-asetuksen termistön mukaan ”rekisteröityjen”) että kansallisen lainsäädännön vaatimukset henkilötietojen käsittelylle ovat tiukentuneet.

Viranomaisten henkilötietojen käsittely perustuu virastojen lakisääteisiin tehtäviin. Henkilötietojen käsittelyn tarkoitukset ja keinot määritellään lainsäädännössä, kun on kyse viranomaisista. Kaikessa henkilötietojen käsittelyssä on kyettävä perustelemaan käsittelyn tarkoituksenmukaisuus sekä osoittamaan tiedon käsittelyn käyttösidonnaisuus ja se, että tiedon minimikäsittelyn eli mahdollisimman vähäisen käsittelyn vaatimukset toteutuvat tiedon elinkaaren hallinnan kautta. (EU:n tietosuoja-asetus, artikla 5; Korpisaari ym. 2018.)

Tietosuoja-asetuksen viidennessä artiklassa kuvataan laajemmin ylemmällä tasolla niitä henkilötietojen käsittelyä koskevia periaatteita, joita tulee myös tietojen siirroissa noudattaa. Asetuksessa mainitaan käsittelyn lainmukaisuus, jonka mukaan tietojen käsittelylle tulee olla laillinen peruste. Samassa artiklassa mainitaan myös käsittelyn kohtuullisuus ja läpinäkyvyys, joissa tulee huomioida rekisteröityjen edut ja odotukset. On myös tilanteita, kun kyseessä on joko rekisterinpitäjän tai kolmannen osapuolien oikeutettu etu, jonka perusteella voidaan henkilötietojen käsittelyä toteuttaa. Tätä ennen on toteutettava tasapainotesti, jonka avulla arvioidaan, onko rekisteröidyn oikeudet painavampia kuin käsittelijän intressi henkilötietojen käsittelyyn. Artikla viidessä kuvatulla käyttötarkoitussidonnaisuudella rajoitetaan, sitä mihin tarkoituksiin henkilötietoja voidaan käyttää ja minimoinnilla rajoitetaan tiedon käsittelyä. Sälytyksen rajoittamisella taas varmistetaan, ettei tietoja säilytetä kauemmin, kun tarpeen. Erityisen tärkeää on varmistua tiedon eheydestä ja luottamuksellisuudesta.

European Data Protection Board (EDPB, 2020) muistuttaa ohjeessaan tietojen minimoinnin periaatteesta: tietoa käsitellään ja siirretään vain käyttötarkoituksen mukaisesti, ei enempää. (Gonzalez Fuster ym. 2021; Johansson 2022.)

Olennaista tietosuoja-asetuksen voimaan astumisessa on, että rekisterinpitäjien lukuun toimivien tietojenkäsittelijöiden tulee kyetä osoittamaan rekisteröidyille, rekisterinpitäjille sekä valvoville viranomaisille näyttöä siitä, että henkilötietojen käsittely-ympäristö täyttää sille asetetut hallinnolliset-, fyysiset ja tekniset tietoturvavaatimukset (Kaivola 2016).

Tietosuojan kannalta merkityksellisiksi tiedoiksi katsotaan ne henkilötiedot, joita tietojärjestelmät tarvitsevat ylipäätään toimiakseen. Tästä esimerkkinä ovat käyttöjärjestelmien, tietojärjestelmien ja sovellusten tarvitsemat käyttäjätunnus–salasana-yhdistelmät. Eri järjestelmät vaativat eri määrän henkilötietoja toiminnan varmistamiseksi. Tiedoilla ylläpidetään tietoturvaa ja selvitetään ongelmien vianmäärityksiä, ja niitä käytetään hyväksi tuotekehityksessä. Ne myös sisältävät pääsääntöisesti yksilöiviä henkilötietoja, tai tietoja yhdistämällä on mahdollista yksilöidä henkilö. Kyseiset luovutetut henkilötiedot jäävät tietojärjestelmien rekistereihin sekä lokeihin ja ovat näin ollen myös kolmansien osapuolten saatavilla.

Digitalisaation tuomat haasteet muuttavat organisaatiokulttuuria, ja sillä on vaikutusta henkilöstön käyttäytymiseen ja ajattelutapaan (Vaara 2019). Kaikkia muutoksia ei kyetä hahmottamaan, saati sitten niiden vaikutuksia, mikä lisää oletusarvoisen ja sisäänrakennetun tietosuojan tarpeellisuutta. Jatkossa on kyettävä tuottamaan aiempaa parempi valmius tehdä tarvittavia muutoksia, ja on myös tunnistettava heikot signaalit ja osattava reagoida niihin sekä ennaltaehkäisevästi että proaktiivisesti myös tietosuojatyössä (Impiö 2021).

Organisaatiot joutuvat sopeutumaan digitalisaation tuomiin haasteisiin. Esimerkiksi pilvipalveluiden toimittajien säännönmukaiset päivitykset saattavat johtaa suuriin teknisiin muutoksiin, joilla on väistämättä niin suuri vaikutus henkilötietojen käsittelyyn, että se on merkityksellistä rekisteröidyn oikeuksien kannalta. Päivityssykli on usein myös niin hektinen, etteivät aiempien tietoturva-auditointien tulokset enää välttämättä ole valideja. Soinisen (2021) mukaan muutosten rooli on merkittävä, koska niitä tapahtuu ympärillämme jatkuvasti useista eri syistä ja ne myös edellyttävät jatkuvaa reagointia organisaatioissa.

Tietosuoja itsessään ei tarjoa menetelmiä tai välineitä ei-toivottujen, henkilötietojen käsittelyyn kohdistuvien poikkeamien haltuun saamiseksi, vaan tietosuojatyössä turvaudutaan hallinnollisiin, fyysisiin ja teknisiin tietoturvakontrolleihin. EU:n tietosuoja-asetuksen mukaan tietosuojavaatimuksia implementoitaessa hyödynnetään tietoturvakontrolleja, joita kuvataan mm. ISO/IEC 27000 -standardisarjassa, joka tarjoaa suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin. (Siponen 2000.) Tietoturvakontrolleilla tarkoitetaan palveluprosessiin määriteltyjä ja rakennettuja tarkistuspisteitä, joilla havaitaan virheet. Tietoturvakontrolleilla luodaan mahdollisuudet toiminnan seuraamiseen ja kehittämiseen sekä sovellusten ja palveluprosessien laadun parantamiseen. (Lähdesmäki 2020.)

Esimerkkinä tietosuojan ja tietoturvan kiinteästä kytköksestä voidaan pitää tietoturvavalvomoissa syntyvien poikkeamaraporttien hyödyntämistä tietosuojatyössä. Poikkeamatilanteiden analyysissa tulee myös arvioida, miten poikkeama kohdistuu henkilötietoihin. On selvitettävä, miten poikkeamatieto saavuttaa johdon, miten johdolle tuotetaan näistä raporteista ymmärrettävää tietoa ja miten se esitetään. Lisäksi on kysyttävä, onko tieto relevanttia johdon näkökulmasta, mihin toimenpiteisiin se johtaa ja onko toimintamallit kuvattu strategisen johtamisen näkökulmasta.

Tietosuojatyössä mm. tietoturvaan liittyvät poikkeamaraportit voidaan määritellä datamassaksi, jonka asiantuntija jalostaa informaatioksi. Tätä tuotetaan tiedon lähteeksi ja päätöksenteon tueksi organisaation eri tasoille, johtoa myöten. Ennaltaehkäisyn näkökulmasta tieto on arvokasta silloin, kun sen perusteella kyetään arvioimaan poikkeamien mahdollinen vaikutus toimintaan ja osataan estimoida uhan todennäköisyys mahdollisimman varhain, mieluiten jo ennen kuin teknologia siirretään tuotantoympäristöön. Loogisesti tarkasteltuna, tämän tulisi johtaa ennaltaehkäiseviin toimenpiteisiin.

Yhtenä riskin todennäköisyyden arviointikeinona on riskien heikkojen signaalien (weak signals) ja varhaisten varoitusten (early warnings) seuraaminen. Näiden avulla on mahdollista arvioida ei-toivotun tilanteen eskaloitumisen todennäköisyys sekä löytää siihen hallintakeinot. (Immonen & Rantanen 2013; Kaivo-oja 2021.)

Nykyisessä tietosuoja- ja tietoturvatyössä poikkeamiin reagoidaan uhan konkretisoitumisen jälkeen. Tyypillisesti viranomaiset pyrkivät, usein asiantuntijoiden eksplisiittisen tiedon sekä kokemusten kautta syntyneen hiljaisen tiedon avulla, saamaan poikkeavan tilanteen haltuunsa hyödyntämällä tilanteissa syntyvää fragmentoitunutta dataa uhan ollessa jo konkretisoinut, mikä johtaa valitettavan usein monimutkaisten ja toisiinsa vaikuttavien tapahtumasarjojen osaoptimointiin. Ei-toivotut poikkeamat saattavat pitkään jatkuessaan muodostaa organisaatiossa kriisin. Kuten kriisinhallintateorioissa sanotaan, vaikuttavinta kriisinhallintaa on niiden ennaltaehkäisy, jolloin on perusteltua hakea toimintamalleja kriisinhallinnan teorioista (Immonen & Rantanen 2011). Kriisinhallinnan logiikka (ks. luku 5) on rinnastettavissa sisäänrakennetun ja oletusarvoisen tietosuojan vaatimuksiin siitä, että tietoturvatyön on oltava proaktiivista, ennakoivaa ja läpinäkyvää. Myös tietosuojapoikkeamia edeltävissä tilanteissa voidaan tunnistaa heikkoja signaaleja ja varhaisia varoituksia ennen varsinaisen poikkeaman esilletuloa. Kun toiminnan painopistettä siirretään preventioon, kyetään todennäköisyyksien arvioinnin perusteella proaktiivisesti ennaltaehkäisemään ei-toivottuja skenaarioita.

Suomessa konkreettinen esimerkki on lokakuussa 2020 julkiseksi tullut henkilötietovuoto, jossa varastettiin Vastaamo-yrityksen potilastietojärjestelmän tietokanta, noin 10 gigatavua, jossa oli arviolta 33 000 psykoterapiapotilaan tiedot. Tapaus eskaloitui niin laajalle, että valtioneuvosto aloitti siitä lokakuussa 2020 oman selvityksen. Tapauksen vuoksi Vastaamon silloisen toimitusjohtajan omaisuutta takavarikoitiin yli 10 miljoonan euron edestä. (Ralston 2020.)

Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) totesi valvonnan tulosten perusteella, että Vastaamo oli laiminlyönyt yksityisestä terveydenhuollosta annetun lain mukaisia velvollisuuksiaan. Vastaamon potilasasiakirjamerkinnät osoittautuivat tarkastetun otoksen perusteella kirjaviksi ja osin puutteellisiksi. Potilastietojärjestelmä ei lainkaan ohjannut yhdenmukaiseen kirjaamiseen – ohjeita ei ollut ja koulutus ja perehdytys olivat riittämättömiä. Potilastietoihin oli myös liitetty sinne sisällöltään kuulumattomia asiakirjoja. Potilastietojärjestelmässä olevien potilasasiakirjojen tallennusratkaisu ei vastannut arkistolain mukaista pitkäaikaissäilytyksen vaatimusta. Valvira antoikin Vastaamolle määräyksen päivittää potilasasiakirjojen pitkäaikaissäilytys vaatimusten mukaiseksi.

Pakkalan (2021) mukaan Vastaamo oli jo ennen tietomurtoa saanut palveluun tyytymättömiltä asiakkailta muistutuksia, mutta se ei ollut kaikilta osin noudattanut niiden käsittelyssä ja niihin vastaamisessa Valviran ohjeistusta. Muistutusten perusteella terveydenhuollon palveluista vastaavan johtajan olisi pitänyt havaita ja nostaa esiin henkilöstön lisäkoulutus- ja muita kehittämistarpeita. Muistutusten määrä oli kuitenkin kohtuullinen toiminnan laajuuteen nähden. (Pakkala 2021.)

Kaikki valvonnassa ilmenneet poikkeamat olisi asianmukaisella seurannalla kyetty tunnistamaan varhaisiksi varoituksiksi potentiaalisesta poikkeamatilanteesta, ja potilastietojärjestelmään olisi ollut mahdollista tehdä korjaustoimia ennen katastrofin syntymistä.

Rekisteröidyn oikeuksien toteutuminen on EU:n tietosuoja-asetuksen merkittävin vaatimus. Valtorissa tietosuojatyön tavoitteena on yksiselitteisesti vaalia näitä oikeuksia. Tietosuojatyössä kiinnitetään erityistä huomiota tietosuoja-asetuksen viidennessä artiklassa kuvattuihin tietosuojaperiaatteisiin: lainmukaisuuteen, kohtuullisuuteen ja läpinäkyvyyteen, käyttötarkoitussidonnaisuuteen, tietojen minimointiin, täsmällisyyteen, säilytyksen rajoittamiseen sekä eheyteen ja luottamuksellisuuteen. (Tietosuoja-asetus 2016/679.)

Alankomaiden valtion asiantuntijat ovat ansiokkaasti arvioineet, miten hyvin kansainväliset pilvipalvelut täyttävät EU:n tietoturva-asetuksen vaatimukset. Alankomaat on resursoinut Microsoft-asiantuntijoita käymään läpi Microsoftin pilvipalveluita ja arvioimaan niiden yhteensopivuutta EU:n tietosuoja-asetuksen kanssa. Tehty tietosuojan vaikutusten arviointi (DPIA) sekä kolmannen osapuolen pilvipalveluihin kohdistamat ulkopuolisten toteuttamat auditoinnit antoivat alankomaalaisille selkänojan lähteä neuvottelemaan pilvipalveluiden käyttöehtojen päivittämisestä (Wachter & Mittelstadt 2019). Tiivistetysti sanottuna prosessi oli pitkä ja monimutkainen ja vaati mm. Alankomaiden pääministerin sitouttamista neuvotteluihin. Arvioinnin perusteella rekisteröidyn oikeudet ovat tietosuoja-asetuksen viitekehyksestä todennäköisesti uhattuna käytettäessä yhdysvaltalaisia pilvipalveluita. Euroopassa eri toimijoilla on kollektiivinen huoli siitä, miten kansainväliset pilvipalveluiden tarjoajat saadaan vastaamaan tietosuoja-asetuksen vaatimuksiin (Hague Forum for Cloud Contracting 2019).

Syksyllä 2019 Alankomaiden oikeusministeriö toi esiin, että pilvipalveluiden henkilötietojen käsittelyssä ja EU:n tietosuoja-asetuksessa on merkittäviä ristiriitaisuuksia. Kriittisimmäksi haasteeksi koettiin se, että yhdysvaltalaiset

palveluntarjoajat noudattavat lähtökohtaisesti Yhdysvaltojen lainsäädäntöä (mm. Cyber security act, ePrivacy, US Patriot act), jonka määräykset poikkeavat EU:n tietosuoja-asetuksen määräyksistä (EU kansalaisia voidaan vakoilla ilman yksilöön kohdistuvaa etsintälupaa). Kyseinen haaste on ajankohtainen useassa EU:n jäsenmaassa ja EU:n alueella toimivassa kansainvälisessä organisaatiossa. Moni taho tuntee olevansa liian pieni toimija voidakseen neuvotella suurten pilvipalveluiden toimittajien kanssa käyttöehtojen päivittämisestä niin, että pilvipalvelut kirjaimellisesti vastaisivat EU:n tietosuoja-asetuksen vaatimuksia. (Esim. Van den Berg 2019.)

Haasteen juurisyy tuntuu olevan se tosiasia, että Yhdysvalloissa kynnys henkilötietojen luovuttamiseen kolmansille osapuolille yleisen turvallisuuden vuoksi on merkittävästi matalampi kuin EU-alueella. EU:n tietosuoja-asetuksen viitekehyksestä arvioituna rekisteröidyn oikeudet ovat todennäköisesti uhattuna.

Kun pilvipalveluita otetaan käyttöön, EU:n tietosuoja-asetuksen vaatimusten mukaan henkilötietojen käsittelyn vastuu on rekisterinpitäjällä. Rekisterinpitäjän tulee tehdä tarvittavat vaikutusten- ja riskinarvioinnit artiklan 35 mukaisesti niiden hallintakeinojen hyväksyntää varten (Tietosuoja-asetus 2016/679). Rekisterinpitäjä on toimija, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot lakisääteisten velvoitteiden perusteella. Viranomainen ei näin ollen voi itse määritellä henkilötietojen käsittelyn tarkoituksia, vaan se perustuu lakiin. Laissa säädettyä käsittelyn tarkoitusta noudattaa ja toteuttaa kukin viranomainen omalta osaltaan.

Näiden reunaehtojen perusteella rekisterinpitäjä määrittelee henkilötietojen käsittelyn vaatimukset. Rekisterinpitäjä ja tietojenkäsittelijä sopivat yhteisesti tietojenkäsittelyn periaatteista. Kaikkien toimijoiden – pääkäsittelijän ja alikäsittelijöiden, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun –, tulee kyetä osoittamaan, että tietoja käsitellään rekisterinpitäjän vaatimusten mukaisesti. (Tietosuoja-asetus 2016/679.)

Tarkasteltaessa riskejä ylätasolla on jo tunnistettu yhdeksi fundamentaaliseksi tosiasiaksi, että pilvipalvelut mahdollistavat henkilötietojen virtaamisen EU-alueen ulkopuolelle. Tällöin tietojenkäsittelyssä ei noudateta EU:n tietosuoja-asetuksen vaatimuksia (Van den Berg 2019; Calvi 2022). Tästä seuraa, että on arvioitava myös henkilötietojen käsittelyyn liittyvä tiedon elinkaaren hallinta, exit-strategia (miten tiedot siirretään järjestelmästä toiseen), palvelun saavutettavuuteen ja käytettävyyteen liittyvät riskit sekä toimittajariippuvuuteen liittyvät riskit suhteessa rekisteröidyn oikeuksiin. Tässä luvussa aihetta tarkastellaan keskeisten käsitteiden, teorioiden ja lainsäädäntöjen kautta.

2.1 Yksityisyys käsitteenä ja lainsäädäntö

Ajatuksen yksityisyydestä ihmisen perusoikeutena katsotaan yleisesti saaneen sille kuuluvaa painoarvoa 1890-luvulla Yhdysvalloissa vastalauseena lehdistön toimille, joissa raportoitiin kansalaisten yksityiselämästä julkisesti. Kaksi

lakimiestä, Samuel Warren ja Louis Brandeis, kirjoittivat artikkelin The Right to Privacy, joka julkaistiin vuonna 1890 Harvard Law Review'ssa. Artikkelissa korostettiin ajatusta ihmisten oikeudesta olla yksin tai omassa rauhassa (the right to be alone) (Korhonen 2003, 79–80; Razdan 2013).

Yhdistyneiden kansakuntien vuoden 1948 Ihmisoikeuksien yleismaailmallisen julistuksen 12. artiklan mukaan kenenkään yksityiselämään ei saa mielivaltaisesti puuttua eikä mainetta tai kunniaa loukata ja jokaisella on lain suoja tällaista loukkausta vastaan (Nyst & Falchetta 2017). Euroopan ihmisoikeussopimuksen (1953) 8. artiklan mukaisesti jokaisella on oikeus nauttia yksityis- ja perhe-elämän kunnioitusta, johon viranomaiset voivat puuttua vain lain niin salliessa.

Euroopan neuvoston tietosuojasopimuksessa on ensimmäinen tietosuoja-alan oikeudellisesti sitova kansainvälinen väline, määritellään perusperiaatteet, joihin sopimuksen hyväksyneet osapuolet sitoutuvat yksityisyyden suojaamiseksi henkilötietojen automaattisessa tietojenkäsittelyssä (Henkilötietolaki 1999/523; Korhonen 2003, 93).

Suomessa tietosuojasopimuksen asettamat vaatimukset toteutuivat Suomen henkilörekisterilain (471/1987) astuttua voimaan. Jo tässä yhteydessä alkoi muotoutua yksi nykyisen EU:n tietosuoja-asetuksen keskeisimmistä tavoitteista sisäänrakennetun ja oletusarvoisen tietosuojan näkökulmasta: hyvän henkilötietojen käsittelyn kautta tapahtuva yksityisyyden suojan loukkauksen ennaltaehkäisy.

Yksityisyyden käsite on moniulotteinen, ja sen merkitys vaihtelee eri kulttuureissa sekä muuttuu yhteiskunnan ja teknologian kehityksen mukana. Henkilötietojen tehokkaan keräämisen ja hyödyntämisen nähdään usealla eri tavalla olevan tärkeässä roolissa yhteiskunnan kehityksen kannalta. Viime vuosien aikana onkin syntynyt uusia menetelmiä ja teknologioita, jotka kykenevät yhä tehokkaammin prosessoimaan yhä suurempia ja hajautuneempia tietomassoja (Hokkanen 2015). Yksityisyyden merkitys ja tärkeys nousevat esille siinä, että tietosuoja-asetus korostaa rekisteröidyn oikeuksia, rekisterinpitäjän velvollisuuksia, viranomaisvaltuuksia, EU:n yhteistä tietosuojakehitystä sekä digitaalisten sisämarkkinoiden kehitystä (Kaivola 2016).

Yksityisyyteen liittyy monia konkreettisia teemoja puolesta ja vastaan. Tänä päivänä on esitetty argumentteja siitä, että yksityisyys ja yleinen turvallisuus sulkisivat toisensa pois (Telaranta 2017). Yleisen turvallisuuden takaamiseksi on joissakin yhteiskunnissa kynnys henkilötietojen luovuttamiseen kolmansille osapuolille matalampi kuin toisissa. Yksityisyyden ja kansallisen turvallisuuden suhteen määrittely ei ole helppoa. Tehdyissä tiedonsiirtoja koskevissa riskinarvioinneissa (TIA) nousee selkeästi esille, että tietosuojalainsäädännöt poikkeavat suuresti eri maissa ja turvallisuusviranomaisten toimivaltuuksissa on suuria eroja eri valtioiden välillä. Tämä on noussut esille yhtenä keskeisimpänä esteenä pilvisiirtymälle. (Sotto ym. 2010; Furramani & Ozpozan 2023.)

Tietosuoja pilvipalveluissa näyttääkin muodostuvan turvallisuuden, taloudellisen näkökulman ja yksityisyyden suojan väliseksi debatiksi. Käsillä olevaa ilmiötä on syytä tarkastella edellä mainituista viitekehyksistä. Toisaalta

teknologiana ja investointina pilvipalvelut tunnistetaan kustannustehokkuudeltaan sekä käytettävyysominaisuuksiltaan loppukäyttäjiä tyydyttäväksi IT-ratkaisuksi. Tietosuoja-asetuksen vaatimusten näkökulmasta pilvipalveluiden käyttöönotossa on kuitenkin havaittu olevan riskejä. Modernissa tietoyhteiskunnassa tietoverkkoja käytetään niin hyvään kuin pahaankin, joten turvallisuusviranomaiset tarvitsevat työkaluja rikosten ja turvallisuusuhkien ennaltaehkäisyyn sekä tapahtumien tutkintaan ja vaikuttamiseen kybermaailmassa.

Osana Euroopan unionin tietosuojalainsäädännön uudistusta muuttui henkilötietojen käsittelyn luonne merkittävästi myös Suomessa, kun yleinen **EU:n tietosuoja-asetus (GDPR)** tuli voimaan 24. toukokuuta 2016. Tietosuoja-asetusta alettiin soveltaa kahden vuoden siirtymäajan jälkeen 25. toukokuuta 2018 alkaen. Asetuksen mukaan tietosuojalla tarkoitetaan yksilön yksityisyyden turvaamista henkilötietojen käsittelyn eri menetelmin ja niiden suojaamista toteuttamalla käsittelyssä eri tietoturvakontrolleja. EU:n tietosuoja-asetus takaa yksilöille oikeuden päättää omien henkilötietojensa käsittelystä ilman kenenkään oikeudetonta puuttumista siihen. Poikkeuksena ovat viranomaisten lakisääteisiin velvoitteisiin liittyvien henkilörekisterien ylläpito ja tietojenkäsittely. Tietosuoja on yhtäältä henkilön oikeutta omiin tietoihinsa ja toisaalta kaikkien muiden tahojen velvollisuutta toimia siten, että tämä oikeus myös toteutuu. Tietosuoja-asetus ei kuitenkaan kuvaa keinoja, joilla vaatimuksia voidaan toteuttaa. Konkreettiset keinot tietojen suojaamiseksi kuvataan eri tietoturvastandardeissa, VAHTI-ohjeissa sekä eri kriteeristöissä. (Valtiovarainministeriö 2016.)

Tietosuoja-asetuksen tärkeimpänä tavoitteena on Euroopan unionin yksittäisen kansalaisen tietosuojan parantaminen. Tietosuoja-asetuksen vaatimuksilla tietojen turvallisesta säilyttämisestä ja oikeista toimintatavoista pyritäänkin edesauttamaan sitä, että henkilötietojen käsittelijät, esimerkiksi kansainväliset verkkokaupat, käsittelevät henkilötietoja läpinäkyvästi ja asianmukaisesti. Tietojenkäsittelijöiden pitää selkeästi osoittaa, miten tietoja käsitellään sekä millä tietoturvakontrolleilla varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys. (Lehtinen 2010; Puhakka 2021.)

Tietosuoja-asetuksen yhtenä tarkoituksena on ajantasaistaa tietosuojaa koskevaa sääntelyä, jotta teknologian kehitykseen ja globalisaatioon liittyviin henkilötietojen suojan haasteisiin voidaan vastata. Asetuksen tarkoituksena on myös tukea digitaalitalouden kehitystä sisämarkkinoiden alueella yhdenmukaistamalla jäsenvaltioiden tietosuojaa koskevat säännökset. Kaiken kaikkiaan tietosuoja-asetuksen tarkoituksena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. (Valtiovarainministeriö 2016.)

Tietosuoja-asetusta täydentävä uusi **kansallinen tietosuojalaki** hyväksyttiin marraskuussa 2019 eduskunnassa, ja tasavallan presidentti vahvisti lain 5. joulukuuta 2019. Tietosuojalaki ei muodosta itsenäistä ja kattavaa sääntelykokonaisuutta, vaan sitä sovelletaan rinnakkain asetuksen kanssa. Uudella tietosuojalailla säädetään tietyissä kysymyksissä poikkeuksia ja täsmennyksiä EU:n tietosuoja-asetukseen. Tietosuojalailla säädetään myös valvontaviranomaisesta sekä eräistä henkilötietojen käsittelyyn liittyvistä erityistilanteista, kuten

sananvapauden ja henkilötietojen suojan yhteensovittamisesta. Lain voimaan tultua kumottiin henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. (Valajärvi 2020.)

Myös monet **muut lait** ohjaavat tietosuojaa ja rekisterinpitäjän toimintaa. Sellaisia ovat mm. laki sähköisen viestinnän palveluista, tiedonhallintalaki sekä yksityisyyden suojasta työelämässä annetussa laissa.

Sähköisten viestinnän palveluita koskevan lain (917/2014) tavoitteena on edistää sähköisen viestinnän palvelujen tarjontaa ja käyttöä. Tavoitteena on myös turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suoja.

Julkisen hallinnon tiedonhallinnasta annetulla lailla (906/2019), jäljempänä tiedonhallintalaki, varmistetaan viranomaisten tietoaineistojen yhdenmukainen hallinta ja tietoturvallinen käsittely. Valtion virastot, laitokset ja liikelaitokset ovat lain tarkoittamia tiedonhallintayksiköitä. Laissa säädetään myös viranomaisten tietojärjestelmien välillä tapahtuvasta tietojen sähköisestä luovuttamisesta. Tietoja luovuttava taho varmistaa luovutettavien tietojen tarpeellisuuden tai välttämättömyyden tietoja saavan viranomaisen tehtävien hoitamiseksi. Usean viranomaisen ollessa kyseessä tämä tehdään toimialasta vastaavan ministeriön johdolla. Sääntelyllä pyritään tehostamaan viranomaisten tiedonhallintaa, jotta viranomaiset voivat tarjota palveluja hyvää hallintoa noudattaen laadukkaasti ja hoitaa tehtävänsä tuloksellisesti.

Yksityisyyden suojasta työelämässä annetun lain (759/2004) 3 §:n mukaan työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin. Lisäksi 5 §:ssä säädetään terveydentilaa koskevien tietojen käsittelystä. (Yksityisyyslaki 759/2004.) Suomessa tietosuojatyötä valvovat tietosuojavaltuutetun toimisto sekä Liikenne- ja viestintävirasto Traficom.

Tietosuojavaltuutettu valvoo tietosuoja-asetuksen sekä siihen liittyvän kansallisen tietosuojalain noudattamista. Tietosuojavaltuutettu valvoo lisäksi osittain sähköisten viestinnän palveluita koskevan lain säännösten noudattamista yhdessä Traficomin kanssa. Tietosuojavaltuutetun toimivaltaan kuuluu tarvittaessa antaa rekisterinpitäjille ja henkilötietojen käsittelijöille laajasti määräyksiä.

Liikenne- ja viestintävirasto Traficom valvoo sähköisen viestinnän palvelulain noudattamista. Traficomilla on laajat toimivaltuudet lain noudattamisen valvonnassa; se antaa esimerkiksi huomautuksia ja korjausvelvoitteita lain rikkomisesta sekä väliaikaisia päätöksiä vakavaa haittaa aiheuttavan toiminnan keskeyttämisestä.

2.2 Tietoturvallisuus käsitteenä

2.2.1 Tietosuoja

Tietosuojalla (data protection) tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista rekisteröidyn yksityisyyden, oikeuksien ja

oikeusturvan varmistamiseksi. Tietosuojan tarkoituksena on tiedon kohteen (data subject) yksityisyyden, etujen sekä oikeusturvan turvaaminen. Viranomaisten henkilötietojen käsittelyllä viitataan velvollisuuksiin, jotka koskevat viranomaisten ja yksityisten tahojen ylläpitämiä henkilörekistereihin sisältyviä tietoja, sekä muita määräyksiä, kuten rekisteröidyn oikeuksia. (Tietosuoja-asetus 2016/679; Kaivola 2016.) Arjessa tämä merkitsee henkilötietojen käytön ja muun käsittelyn seurantaa ja valvontaa. Siihen kuuluvat mm. asiakastietojen luvattoman käsittelyn estäminen, asianmukaiset lokijärjestelmät, henkilötietojen käytön seurannan ja valvonnan vuosisuunnitelman laatiminen, hyväksyminen ja seuranta sekä asiakastietojen käsittelyn suunnitelmallinen, säännöllinen ja ulospäin uskottava jälkikäteisvalvonta.

Rekisteröity on kaikessa yksinkertaisuudessaan henkilö, jonka henkilötietoja käsitellään (Korpisaari ym. 2018).

Henkilötiedoilla tarkoitetaan kaikkia niitä henkilöä tai hänen ominaisuuksiaan koskevia merkintöjä, joiden avulla hänet, hänen perheensä tai hänen kanssaan yhteisessä taloudessa elävät voidaan tunnistaa. Käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa, henkilötietoja sisältävää tietojoukkoa kutsutaan puolestaan **henkilörekisteriksi**. (Kleemola 1998, 6; Junttila 2013.)

Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjällä on ensisijainen vastuu tietosuoja-asetuksen noudattamisen varmistamisesta ja sen osoittamisesta. Rekisterinpitäjän vastuulla on määritellä henkilötietojen käsittelyn tarkoitus ja keinot, jolla tarkoitetaan tiedon käyttösidonnaisuutta sekä sen minimikäsittelyn periaatteita. (Kaivola 2016).

Tietosuoja edellyttää tietosuoja-asetuksen mukaan rekisterinpitäjältä teknistä ja organisatorista toteutustapaa suunnittelusta käsittelyvaiheeseen. Käytännössä se tarkoittaa sitä, että otettaessa tietojärjestelmiä valtionhallinnossa käyttöön tulee korostetusti huomioida henkilötietojen käsittelyn tarkoituksenmukaisuus, minimikäsittelyn vaatimukset sekä tiedon elinkaaren hallintaan liittyvät kysymykset. (Kaivola 2016.) Se määrittelee myös käsiteltävät henkilötiedot, rekisteröityjen ryhmät, käsittelyn oikeusperusteen, kolmannet osapuolet, joille henkilötietoja luovutetaan tai siirretään, rekisteröityjen oikeuksien toteuttamisen ja tietojen säilytysajat. (Valtiovarainministeriö 2016; Tietosuoja-asetus 2016/679; Kaivola 2016.)

Tietojenkäsittelijä säilyttää ja käsittelee henkilötietoja rekisteripitäjän lukuun, jolloin tietojen käsittelyoikeus on riippuvainen rekisterinpitäjästä. Oikeus tietojen käsittelyyn perustuu rekisterinpitäjän kanssa tehtävään tietojenkäsittelysopimukseen sekä rekisterinpitäjän antamaan ohjeistukseen. Tietosuoja-asetuksen 28. artiklan perusteella tietoja saa käsitellä ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti eikä tietoja voi käsitellä omiin tarkoituksiin. Tietojenkäsittelijälle on kuitenkin jätetty jossain määrin mahdollisuus vaikuttaa käsittelyn keinoihin ilman, että toimintaa tulkittaisiin rekisterinpitäjyydeksi. Hän voi päättää esimerkiksi IT-järjestelmien ja tietojen siirtoon käytettävistä

menetelmistä, tietoturvaa koskevista yksityiskohdista sekä säilytysaikojen ja poistamisen käytännön toimeenpanosta. (Valtiovarainministeriö 2016; Tietosuoja-asetus 2016/679; Kaivola 2016.)

Tietojen alikäsittelijä toimii tietojenkäsittelijän eli pääkäsittelijän alihankkijana, joka on osallisena henkilötietojen käsittelyprosessissa. Tietojenkäsittelyssä alikäsittelijöitä koskevat samat velvollisuudet kuin pääkäsittelijää suhteessa rekisterinpitäjään.

Henkilötietojen käsittelyllä tarkoitetaan kaikenlaisia toimintoja, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen. (Valtiovarainministeriö 2016.)

Käsittelyllä tarkoitetaan tiedon, lokitiedon, tietoaineiston tai asiakirjan vastaanottamista, laatimista, keräämistä, järjestämistä, jäsentämistä, tallentamista, katselua, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, luovuttamista, kopiointia, siirtoa, välittämistä, tuhoamista, säilyttämistä, arkistointia ja muita tietoon tai asiakirjaan kohdistuvia toimenpiteitä. (Valtiovarainministeriö 2016.)

Henkilötietojen tietoturvapoikkeamalla ja **tietoturvaloukkauksella** tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää tai muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. (Valtiovarainministeriö 2016.)

Taksonomialla eli tietorakenteiden luokittelujärjestelmillä tietoa järjestetään luokkiin ominaisuuksiensa perusteella hierarkkisesti. Se selkeyttää tiedon hallintaa ja käyttöä. Yhteisen taksonomian muodostaminen on merkityksellistä henkilötietojen käsittelyn vastuiden ja velvoitteiden määrittelemisen kannalta, mutta yleisesti hyväksyttyä tapaa henkilötietojen jaotteluun ei ole vielä käytössä.

Kuviossa 1 esitetään Alankomaiden oikeusministeriön tekemä henkilötietojen jaottelu, jota hyödynnetään tässä tutkimuksessa määriteltäessä henkilötietojen käsittelyn rooleja, vastuita sekä velvoitteita. Henkilötiedot on jaettu kolmeen luokkaan: sisältötiedot (content data), metatiedot eli käyttötiedot (functional data) sekä diagnostiikkatiedot (diagnostic data).

KUVIO 1. Henkilötietojen jaottelu: sisältötiedot, käyttötiedot ja diagnostiikkatiedot

Sisältötiedoilla tarkoitetaan käsiteltäviä, tallennettuja tai lähetettyjä henkilötietoja, jotka ovat erilaisissa tiedostoissa, kuten dokumenteissa, taulukoissa ja sähköpostien sisällöissä. Tähän luokkaan pilvipalvelutoimittajilla on tarjottavana salaus- ja pseudonymisointiratkaisuja. Kahdessa muussa luokassa henkilötietojen käsittelyn hallinta on haasteellisempaa, koska yksilöivä henkilötieto on tunnistettavissa selväkielisenä ja jäljitettävissä rekisteröityyn.

Käyttö- tai metadataan kuuluvat ne henkilötiedot, joita järjestelmät tarvitsevat, jotta ne ylipäätään toimivat. Tyypillisimmin tietotekniikkaratkaisujen toimittajat määrittelevät tarvitsevansa näitä tietoja palveluiden tuottamiseen ja toteuttamiseen, asiakasviestintään, laskuttamiseen sekä mainonnan ja markkinoinnin kohdistamiseen.

Diagnostiikkatiedoilla tarkoitetaan tietoja, joita käytetään järjestelmäongelmien, tapahtumien suorituskyvyn, virheiden tai virheellisen tuotoksen tutkimiseen ja diagnosointiin. Toimittajat kuvaavat pakollisiksi diagnostiikkatiedoiksi niitä (vähimmäis)tietoja, joita toimittajien on kerättävä, jotta tuote pysyy suojattuna ja ajan tasalla ja toimii odotetulla tavalla. Kahdessa viimeksi mainitussa luokassa on erittäin vaikea määritellä, kuka toimijoista on rekisterinpitäjä, koska tietotekniikkaratkaisujen toimittajilla on perustelut henkilötietojen käsittelyn tarkoituksiin ja he vastaavat myös keinoista, joilla henkilötietoja käsitellään.

Kun henkilötietojen käsittelyssä määritellään eri toimijoiden rooleja, vastuita ja velvoitteita, jää kaksi viimeisintä luokkaa usein vähäiselle huomiolle, vaikka tosiasiallisesti suurin osa käsiteltävistä henkilötiedoista kuuluu juuri niihin. Tätä luokittelua ei ole verifioinut mikään virallinen taho. Mitä ilmeisimmin tämän vuoksi se ei ole saanut Suomen julkishallinnossa varauksetonta vastaanottoa, vaikkakin yhteisen taksonomian merkitystä korostetaan keskusteluissa.

Henkilötiedoista keskustelemisen vaikeutta lisää myös se, että yhdysvaltalaisilla pilvipalvelutoimittajilla on omat taksonomiansa henkilötiedoille. Heidän

käytössään ovat termit customer data ja service data (tai service generated data). Customer datan voidaan tulkita vastaavan sisältötietoa (content data). Service data vastaa lähinnä kahta muuta luokkaa eli metatietoja (käyttötietoja, functional data) sekä diagnostiikkatietoja (diagnostic data) yhdessä.

Tietosuojan tavoitteena on hyvän käsittelytavan luominen ja toteuttaminen henkilötietojen käsittelyn kaikissa vaiheissa. Tarkoituksena on henkilön oikeuksien kunnioittaminen ja toteuttaminen niin rekisteröidyn kuin rekisterinpitäjänkin näkökulmasta. EU:n tietosuoja-asetuksen (2016/679) sekä kansallisen tietosuojalain (1050/2018) vaatimukset henkilötietojen käsittelystä on otettava huomioon koko niiden elinkaaren ajan (Kaivola 2016). Tavoitteena on ennen kaikkea varmistaa yksityisten henkilöiden eli rekisteröityjen yksityisyys, edut ja oikeusturva. Rekisterinpitäjinä yritysten, järjestöjen, julkishallinnon ja muiden organisaatioiden on pyydettäessä pystyttävä osoittamaan asianmukainen henkilötietojen käsittely (Korpisaari ym. 2018).

Tietosuojatyössä on tiedolla johtamisella potentiaalisesti merkittävä rooli. Tarvetta muuttaa painopistettä kohti ennaltaehkäisyä on kuvattu tietosuoja-artiklassa 25, jossa kuvataan sisäänrakennettua ja oletusarvoista tietosuojaa (Kaivola 2016). Kun tietosuojatyötä tarkastellaan tiedolla johtamisen kannalta, datan lähteinä voidaan pitää rekisteröidyn oikeuksiin, rekisterinpitäjän velvollisuuksiin ja osoitusvelvollisuuteen liittyvää dataa sekä säännöllisiä raportteja, kuten tietotilinpäätöstä ja poikkeamaraportteja. Asiantuntijat, kuten tietoturva-asiantuntijat ja tietosuojavastaavat, muodostavat tästä datamassasta informaatiota erityyppisen tiedon lähteeksi. Tämän informaation tulee olla päätöksentekoprosesseissa yksi tiedon lähde.

Poikkeamien uhasta syntyy huomattava määrä dataa, jota ei näytetä hallittavan strategisessa johtamisessa. EU:n tietosuoja-asetuksessa kuvatun oletusarvoisen ja sisäänrakennetun tietosuojan (privacy by design) yhtenä keskeisenä argumenttina on ennaltaehkäisevien toimenpiteiden tärkeys tietosuojatyössä.

Eri kulttuureissa yksityisyyden suoja saa eri painoarvon, ja sillä on suora vaikutus henkilötietojen käsittelyyn. Nykyisessä tilanteessa, jossa yksityisyyden suojan viitekehyksestä syntyvä ohjeistus henkilötietojen käsittelyyn on nostanut esiin vähintäänkin epäselvyyksiä globaalissa digitaalisessa taloudessa, on julkisuudessa alettu kyseenalaistaa globaalien pilvipalveluteknologian toimittajien suhdetta EU:n tietosuoja-asetukseen.

Huoli henkilötietojen joutumisesta perusteettomasti sellaisten ulkopuolisten toimijoiden haltuun, joille tieto ei kuulu, on ollut läsnä keskusteltassa pilvipalveluiden kehityksestä. Tämä huoli voidaankin nähdä yhdeksi EU:n tietosuoja-asetuksen kulmakiveksi. Viime vuosien aikana on tapahtunut massiivisia henkilötietovuotoja, esimerkiksi mm. Cambridge Analytica -tapaus, jossa yritys keräsi luvatta noin 50 miljoonan yhdysvaltalaisen Facebook-käyttäjän henkilötietoja ja hyödynsi niitä mm. vuoden 2016 Yhdysvaltain presidentinvaalikampanjassa (Kanakia ym. 2019, 1–5).

Toinen esimerkki on johdannossa mainittu kanne Facebookia vastaan, jossa itävaltalainen Max Schrems vaati kieltämään eurooppalaisten tietojen luovuttamisen Yhdysvaltoihin heikon yksityisyydensuojan takia. Se herätti unionin

jäsenmaissa huolen yksityisyyden suojan toteutumisesta pilvipalveluissa ja johti siihen, että Privacy Shield -sopimus, jonka tarkoituksena oli suojata eurooppalaisten henkilökohtaisia tietoja, mitätöitiin yksipuolisesti heinäkuussa 2020. (Johansson 2022.) EU:ssa yksityisyyden suojaan kohdistettaviin vaatimuksiin ovat tietosuojaviranomaisten lisäksi alkaneet kiinnittää huomiota myös kansalaiset, rekisteröidyt. Kritiikin keskiössä ovat nimenomaan suuret globaalit teknologiatoimittajat. (Guardian 2018.)

Monimutkaisten ilmiöiden hahmottamista voi kuvata tarinalla, jossa kolme henkilöä tunnustelee silmät peitettynä elefanttia. Yksi koskettelee häntää, toinen jalkaa ja kolmas kärsää. Tämän perusteella heille muodostuu kovin erilaiset mielikuvat eläimestä. Tietosuojatyössä ollaan hieman saman haasteen äärellä. Jotta saavutetaan ymmärrys, millaisesta kokonaisuudesta on kyse, tulee tietosuojaa tarkastella useasta eri näkökulmasta ja yhdistää ne. Tietosuojan monisyistä haasteellisuutta voisi konkretisoida Rubikin kuutio -vertauksella, jossa yksi kuution seinä vastaa yhden tietosuojan hallintamallin osa-aluetta. Käytännössä siis eri asiantuntijoiden on kyettävä muodostamaan näkemyksensä käytössä olevan datan perusteella, eikä kokonaiskuva ole valmis ennen kuin Rubikin kuution kaikki seinät ovat järjestyksessä. Tähän käytännössä tarvitaan asiantuntijuutta usealta eri alalta, kuten esimerkiksi juridiikan, riskienhallinnan ja tietoturvan aloilta, tulkitsemaan pilvipalveluiden henkilötietovirtoja. Jos organisaation tietosuojan kypsyystaso on heikko, haasteeksi tulee tietosuojan tarkasteleminen kovin kapeakatseisesti. Silloin asiantuntijoiden käytettäväksi ei synny merkityksellistä informaatiota, ja proaktiivinen ja ennaltaehkäisyyn tähtäävä tietosuojatyö tyrehtyy.

Tietosuojan hallintamallin avulla organisaatiot toteuttavat tietosuojaan liittyvää osoitusvelvollisuuttaan sekä rekisteröidyille että tietosuojaviranomaisille. Hallintamalli perustuu ISO 27001 -standardin mukaiseen tietoturvan hallinnan logiikkaan ja koostuu kymmenestä osa-alueesta (kuvio 2). Tietosuojan hallintamalli ja siihen liittyvät työkalut antavat yrityksille keinot tietosuojan jatkuvaan hallintaan ja tilannekuvan ylläpitämiseen (ISO 27001).

KUVIO 2. Tietosuojan hallintamalli, ISO 27001 (ISO/IEC 27001 ja ISO/IEC 27002)

Koska EU:n tietosuoja-asetus on EU:n jäsenvaltioiden yhteisesti hyväksymä, siinä on jouduttu tekemään kompromisseja ja jäsenvaltiot päättävät sen toteutustavoista itse tietyn kansallisen liikkumavaran sisällä (Melto 2019). Tietosuojavaatimuksia täytetään käytännössä pääasiassa juridisella sääntelyllä ja hallinnollisilla, fyysisillä sekä teknisillä tietoturvakontrolleilla. Hallintamalli argumentoi tietosuojan ja tietoturvan välisen yhteyden ja skaalautuu yritysten koon ja tarpeiden mukaisesti. Tietosuoja-asetus korostaa kuitenkin myös riskiperusteista näkökulmaa sekä ennaltaehkäisevää, proaktiivista ja läpinäkyvää tietosuojatyötä. Räätälöitäessä Valtorin hallintamallia ISO-standardista myös viimeksi mainitut vaatimukset pyrittiin tuomaan selkeästi esille.

Tässä tutkimuksessa hallintamalli on muokattu viideksi osa-alueeksi, jotta se vastaa paremmin Valtorin tarpeisiin (kuvio 3) ja antaa keinot ja työkalut hallita tietosuojaa kokonaisuutena. Työssä on varmistettu, että Valtorin tarpeisiin muokattu hallintamalli pitää sisällään ISO 27001 -standardin osa-alueet. Tutkimuksen hallintamallin osa-alueet muodostuvat Valtorin tietosuojan hallintamallista.

KUVIO 3. Valtorin tietosuojan hallintamalli, johdettu ISO 27001 -standardista (Lachaud 2020)

Hallinnollinen tietosuoja sisältää rekisteröityjen oikeudet, organisaation tietosuojastrategian, henkilötietojen käsittelyä koskevat sopimukset, henkilötietojen käsittelyyn liittyvän tietosuojan organisoitumisen (tietosuojaorganisaation roolit, vastuut ja velvoitteet) sekä viittaukset kansalliseen tietosuojaa koskevaan lainsäädäntöön.

Operatiivinen tietosuoja sisältää kaikki ne operatiiviset toimenpiteet, joilla rekisteröityjen oikeuksia toteutetaan. Tällaisia ovat mm. henkilötietojen käyttösidonnaisuus, minimikäsittelyvaatimus ja elinkaaren hallinta sekä poikkeamien ja niiden uhkien hallintaprosessit. Tietosuojassa käytettävä taksonomia on myös osa operatiivista tietosuojaa. Lisäksi operatiiviseen tietosuojaan kuuluvat organisaation tietosuojan viestintä ja koulutus.

Tietosuojan riskienhallinta tarkoittaa ennaltaehkäiseviä toimenpiteitä, joita tehdään riskien, niiden uhkien ja vaikutusten todennäköisyyden arvioinnin perusteella.

Sisäänrakennetulla ja oletusarvoisella tietosuojalla edistetään riskilähtöisesti rekisteröityjen oikeuksien toteutumista seuraaviin periaatteisiin nojautuen:

- oletusarvoinen tietosuoja (privacy by default)
- proaktiivisuus
- ennaltaehkäisy
- vuorovaikutus
- tarkoituksenmukaiset menetelmät
- läpinäkyvyys.

Kanadalainen Ann Cavoukian (2010) esitteli yhdessä Hollannin tietosuojaviranomaisen kanssa **sisäänrakennetun ja oletusarvoisen tietosuojan** (privacy by design, PbD). Ajatus on peräisin jo 1990-luvulta, mutta malli julkaistiin

virallisesti vuonna 2009, ja tietosuoja-ammattilaiset ottivat termin käyttöön vuonna 2010 kansainvälisessä tietosuojan ja -turvan ammattilaisten konferenssissa.

Mallissa tietosuoja jaetaan seitsemään yksityisyyttä parantavaan periaatteeseen. Ensimmäinen periaate on, että tietosuojan on oltava proaktiivista ja ennaltaehkäisevää. Tietosuojan tulee olla ennakoivaa, niin että riskit tunnistetaan etukäteen ja vahinkojen hoitamisen sijasta yksityisyyden loukkaukset ja tietosuojariskit ennaltaehkäistään (Impiö 2021, 24).

Toisen periaatteen mukaan henkilötiedot suojataan tarkoituksenmukaisilla menetelmillä automaattisesti, olivatpa tiedot tietojärjestelmissä tai manuaalisesti käytössä digitaalisessa muodossa. Tällöin puhutaan tietosuojasta oletuksena (privacy by default). Kolmas periaate on hyvin lähellä edellä kuvattua: yksityisyys tulee sisällyttää järjestelmiin niin, ettei käyttäjän tarvitse kiinnittää henkilötietojen käsittelyyn erikseen huomiota eikä etenkään tavalla, joka heikentäisi käytettävyyttä. Tähän liittyy keskeisesti neljäs periaate, jonka tavoitteena on tuottaa lisäarvoa (full functionality). Edistyksellinen käytettävyys ei kumoa yksityisyydensuojaa, eikä järjestelmän turvallisuus kumoa yksityisyyttä. (Cavoukian 2010, 3–4.)

Viidennessä periaatteessa viitataan tietojen suojaamiseen alusta loppuun (end-to-end lifecycle protection). Tätä voidaan kuvata myös termillä tiedon elinkaaren hallinta, jossa tiedon keräämiselle ja käsittelylle on olemassa selvä peruste. Kuudennen periaatteen mukaan tietosuojaprosessien ja -käytäntöjen tulee olla selkeästi ja läpinäkyvästi toteutettuja sekä kaikkien osapuolten saatavilla.

Läpinäkyvyys on myös yksi EU:n tietosuoja-asetuksen viidennessä artiklassa kuvatuista tietosuojaperiaatteista, ja siihen viitataan myös 12. artiklassa puhuttaessa informoinnista. Tietosuojakäytäntöjen tulee olla dokumentoituja, läpinäkyviä ja kaikkien osapuolten saatavilla tarvittaessa. (Kaivola 2016.) Rekisterinpitäjien on huolehdittava siitä, että henkilötietoja käsitellään avoimesti, selkeästi ja ymmärrettävästi.

Seitsemännessä periaatteessa korostetaan rekisteröityjen yksityisyyden kunnioittamista. Käyttäjän kunnioittamisen osatekijät ovat suostumuksen pyytäminen, tietojen täsmällisyys, tietojen saavutettavuus ja toimintojen määräystenmukaisuus (Impiö 2021, 23–28).

Tietosuoja-asetuksen artiklan 25 mukaan rekisterinpitäjän yleisiin velvollisuuksiin kuuluu järjestää sisäänrakennettu ja oletusarvoinen tietosuoja (Kaivola 2016). Sisäänrakennettu ja oletusarvoinen tietosuoja tulee ottaa huomioon sekä henkilötietojen käsittelyn suunnitteluvaiheessa että itse käsittelyn aikana (Korpisaari ym. 2018). Euroopan tietosuojaneuvosto suosittaa ennakoivaa lähestymistapaa. Tietosuojaa on toteutettava tehokkaasti, ja rekisterinpitäjän odotetaan pysyvän ajan tasalla uusimmasta teknologiasta voidakseen taata jatkuvan tehokkaan tietosuojan. Rekisterinpitäjän tulee ottaa huomioon myös toteuttamiskustannukset. Muut huomioon otettavat seikat ovat käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. (Korpisaari ym. 2018.)

Tietosuojan ja tietoturvan välisellä vuorovaikutuksella tarkoitetaan tässä työssä lainsäädännössä määriteltyjen tietosuojavaatimusten toteuttamista fyysisin, hallinnollisin sekä teknisin tietoturvakontrollein.

Tietoturvalla on merkittävä rooli tietosuojaperiaatteiden toteuttamisessa. EU:n tietosuoja-asetus sisältää vaatimukset henkilötietojen käsittelylle, ja sen mukaan tietosuojavaatimusten implementoinnissa hyödynnetään tietoturvakontrolleja. Vuorovaikutus tietosuojan ja tietoturvan välillä syntyy, kun henkilötietojen käsittelylle on määritelty fyysiset, hallinnolliset sekä tekniset kontrollit. Näitä kuvataan mm. ISO/IEC 17799 -standardissa (Siponen 2000). Myös valtiovarainministeriön julkaisema VAHTI-dokumenttisarja sekä Tietoturvallisuuden auditointityökalu viranomaisille, KATAKRI 2015, ovat työkaluja systemaattisen tietoturvan suunnittelussa ja todentamisessa (Päivelin 2019). VAHTI-toiminta on siirtynyt vuoden 2020 alussa valtiovarainministeriöstä Digi- ja väestötietovirastoon.

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) taas on Traficomin Kyberturvallisuuskeskuksen julkaisema kriteeristö, joka tukee valtion toimijoita pilvipalvelujen käyttöönotossa sekä vaatimusmäärittelyiden arvioinnissa (Kosonen 2015).

Suomessa viimeisin tietoturvallisuutta koskeva suositus ja kriteeristö on vuonna 2022 julkaistu Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) (Valtiovarainministeriö 2022).

2.2.2 Tietoturva

Tietoturva tarkoittaa niitä hallinnollisia ja teknisiä toimenpiteitä, joilla toteutetaan tietojen kokonaisvaltaista suojaamista väärinkäytöksiltä, muuttumiselta sekä katoamiselta. Tietoturva kattaa käsitteenä sekä itse tietojen että myös järjestelmien, palveluiden sekä tietoliikenteen suojaamisen. Näillä toimenpiteillä varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen.

Tietoturva koostuu perinteisen jaottelun mukaan kolmesta osa-alueesta: tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Niillä pyritään varmistamaan tietojen, tietojärjestelmien ja palvelujen turvaaminen siten, että tietoturva voidaan taata ja sen voidaan osoittaa toteutuneen.

Luottamuksellisuudella tarkoitetaan, että tieto on vain siihen oikeutettujen saatavilla. Eheydellä tarkoitetaan sitä, että tieto on oikeaa ja eheää eikä se ole muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena. Eheyteen liittyy myös kiistämättömyys eli se, että tietoon tehdyt muutokset sen käsittelyn eri vaiheissa pystytään tarvittaessa todentamaan. Lisäksi tietoturvaan yleisesti liitetään saatavuuden vaatimus, jolla tarkoitetaan sitä, että tieto on saatavilla aina sitä tarvittaessa. (Kosonen 2015.)

Tietoturvalla varmistetaan tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työn resurssit sekä välineistön ja tilojen tietoturvaominaisuudet (Ekman 2022). Erityinen tietoturvaorganisaatio suunnittelee ja toteuttaa tietoa turvaavat toimenpiteet.

Suunnitellessaan kaikkia henkilötietojen käsittelyn vaiheita, joihin kuuluvat hankinta, tarjouspyynnöt, alihankinta, kehitys, tukipalvelut, ylläpito, testaus, säilytys ja poisto, rekisterinpitäjän on huomioitava tietoturvan periaatteen kulmakivet: tiedon eheys, luottamuksellisuus ja saatavuus (Karvi 2010; Laakso 2010; Puhakka 2021).

Tietoturvan tarkoitus on estää tietosuojaloukkaukset sekä edistää henkilötietojen käsittelyn asianmukaista toteutusta, vahvistaa muita periaatteita ja antaa rekisteröityjen saumattomasti toteuttaa asetuksen takaamia oikeuksiaan. Tietosuoja-asetus kehottaa varmistamaan, että uusimman tekniikan mahdollisuudet on otettu huomioon tietosuojaa toteutettaessa. Tämä koskee myös tietoturvaa yhtenä tietosuojan osa-alueena, kun suojataan henkilötietoja. Tietosuoja-asetuksen johdanto-osan kohdan 78 mukaan rekisterinpitäjä voi toteuttaa sisäänrakennettua ja oletusarvoista tietosuojaa muun muassa ”luomalla ja parantamalla turvaominaisuuksia”.

2.2.3 Tietoturvan tavoitteet ja keinot

Tietoturvallisuudella tarkoitetaan tietoliikenne-, laitteisto-, ohjelmisto- ja tietoaineistotoiminnan turvallisuutta, jolla turvataan verkkojen ja palvelujen eheys, luottamuksellisuus ja käytettävyys. Käytännössä tämä merkitsee tietojen, järjestelmien ja palveluiden asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. Tietoturva tarkoittaa siis tekoja ja käytäntöjä, joiden tehtävänä on suojata informaatiota joutumasta vääriin käsiin (Kosonen 2015). Tässä kontekstissa on perusteltua todeta, että tietoturvalla tarkoitetaan niitä hallinnollisia ja teknisiä toimenpiteitä, joilla toteutetaan tietosuojaa, mikä käytännössä tarkoittaa, että tietoturvalla on keskeinen rooli myös osana tietojohtamista.

Tietoturvallisuus on huomattavasti laajempi kokonaisuus kuin pelkästään tietotekniset ratkaisut, ja sen vuoksi kokonaisvastuu tietoturvallisuuden toteutumisesta on aina organisaatioiden johdolla. Johdolla on kuitenkin mahdollisuus delegoida tietoturvallisuuteen liittyviä käytännön tehtäviä osa-alueittain eteenpäin. (Limnéll 2014.) Tietoturvallisuus on prosessi, joka alistetaan jatkuvalle seurannalle. Toiminnan on oltava skaalautuva, geneerinen ja dynaaminen päivityksille, joiden implementoinneille on olemassa strukturoitu suunnitelma. Toiminnan jatkuvuuden kannalta on kriittistä, että toimintaa valvotaan systemaattisesti myös tietoturvapäivitysten jälkeen. (Limnéll 2014.)

Tietoturvallisuus on systemaattinen, strukturoitu prosessi, joka kattaa holistisesti organisaation tiedon hallinnan. Tietoturvallisuus tulee sisällyttää osaksi organisaation toimintaprosesseja, jotta tiedon turvallinen ja asiallinen käsittely toteutuisi käytännön toiminnassa. Tässä prosessinmuutoksessa on tärkeää varmistaa toimijoiden kypsyys ymmärtää tietoturvallisuus osana ammatillista osaamista. Yhtä kriittistä on varmistaa toimintaympäristön kypsyys toteuttaa haluttu

muutos hyödyntäen käyttöön otettavaa teknologiaa. (Wickramasinghe ym. 2009.)

Tietoturvallisuuden standardeista keskeisin on ISO 27000 -sarja, jossa määritellään yleiset vaatimukset tietoturvallisuuden hallintajärjestelmän luomiselle, toteuttamiselle, käyttämiselle, valvonnalle, katselmoinnille, ylläpidolle ja parantamiselle. Standardissa esitetyt yleiset vaatimukset ovat sovellettavissa organisaation tyypistä, koosta tai luonteesta riippumatta. (Brenner 2007.)

Luottamuksellisuudella tavoitellaan sitä, etteivät ulkopuoliset pääse lukemaan salaista tietoa. Tavoitteeseen päästään esimerkiksi salauksen, pääsynvalvonnan, todennuksen, valtuutuksen ja fyysisen turvallisuuden avulla. Lisäksi on huomioitava, että toimijoiden motivaatiolla sekä koulutuksella on yhtä suuri, jollei suurempi, merkitys aineiston luottamuksellisuuden säilymisessä. Eheydellä taataan, ettei tietoon ole tehty luvattomia muutoksia eikä se ole muuttunut satunnaisten virheiden takia. Käytettävyydellä tarkoitetaan sitä, että toimija saa juuri oikean tiedon käyttöönsä sillä hetkellä, kun hänellä on prosessissa sille tarve. Käännettäessä sama asia toisin päin on tiedon käytettävyydessä kyse myös tarpeettoman tiedon välttämisestä. Tiedon eheys ja käytettävyys motivoivat toimijoita käyttämään tarjolla olevaa tietoa suunnitellulla tavalla: he saavat käyttöönsä juuri sen tiedon ja vain sen tiedon, joka on heidän työssään tarpeen. (Wickramasinghe ym. 2009, 150; Koivuharju 2013, 11.)

Tietoturvallisuus tulee juurruttaa osaksi organisaation kokonaisarkkitehtuuria sen kaikilla tasoilla. Vallitsevan kehityksen mukaisesti tietoturvallisuutta tarkastellaan usein teknologisesta viitekehyksestä. Tavoitteena onkin lähestyä tietoturvallisuutta positivismin kautta, jolloin keneltäkään ei suljeta tietoa pois vaan tarvittava tieto on juuri oikeaan aikaan oikeassa paikassa ja oikealla teknologialla käytettävissä, sillä asianosaisella, jolle tieto kulloinkin kuuluu ammatillisen roolin perusteella. Käytännössä tietoturva on siis datan rajaamista pois sellaisilta asiattomilta henkilöiltä, joille data ei kuulu mutta jotka voisivat sen saadessaan muodostaa jonkinlaisen (joko oikean tai vääristyneen) kokonaiskuvan yhdistämällä, tulkitsemalla ja ymmärtämällä kertynyttä tietoa. Organisaatioiden tietoturvallisuuteen liittyviä käytäntöjä ohjaa kaksi keskeistä reunaehtoa: organisaation tavoitteet sekä lainsäädäntö. Näiden perusteella määritellään, miten tietoa tulee käsitellä koko tiedon elinkaaren ajan, jotta toimijat pääsevät kokonaisturvallisuuspolitiikassa asetettuihin tavoitteisiin.

Keskeisimpänä toimenpiteenä prosessissa on määritellä tiedolle omistaja. Tiedon omistajuudelle ominaista on tiedon kontrolloitavuus, jossa ilmenee, kuka on luonut tiedon sekä kuka saa modifioida, arkistoida, jakaa, hyödyntää sekä tuhota tietoa. Lisäksi omistajuus merkitsee oikeutta myöntää muille oikeuksia käyttää tietoa. Keskeistä on ymmärtää tiedon omistajan vastuu tiedoista. Organisaatioiden johdon tehtävänä on vastata siitä, että kaikille tietoaineistoille ja järjestelmille on määritelty omistajat. (Natunen 2014.) Ilman tiedon luokittelua ei synny käsitystä siitä, mitä tietoa on suojattava ja keneltä. Tiedon hyödyntäjän kannalta keskeisempi kysymys on: kuka tarvitsee aineiston käyttöönsä ja millä perustein. Määrittely ja luokittelu ovat aineiston luottamuksellisen käsittelyn

ydin. Yksinkertaistettuna, jos aineistoa ei ole luokiteltu, voidaan kaikki aineisto määritellä julkiseksi, jolloin ei myöskään synny tarvetta tiedon suojaamiselle.

Tiedon elinkaaren hallinnan ratkaisut auttavat hallitsemaan tietomäärän kasvua sekä vaatimukset täyttävää tiedon pitkäaikaista säilyttämistä. Tiedon elinkaaren hallinnan avulla tarkastellaan, mistä tieto on muodostunut, kuka sen omistaa ja kenellä on sen käyttö- ja muokkausoikeudet. Lisäksi on syytä määritellä, miten, kuinka kauan ja missä dataa säilytetään sekä milloin ja miten se aikanaan tuhotaan. Suunnitelmissa on huomioitava tiedon koko elinkaari. Tämä on poikkeuksetta pidempi kuin esimerkiksi prosessit, joissa aineistoa käytetään aktiivisesti. Tiedon elinkaaren hallinta ulottuu tietojärjestelmän kehittämisessä ja testaamisessa syntyvästä datasta tuotantodatan arkistointiin ja aikanaan tiedon tuhoamiseen.

Tiedon elinkaaren hallinnassa on kriittistä huomioida tiedon käyttöoikeuksien lisäksi tiedon tarkoituksenmukainen arkistointi, jolla lyhennetään varmistuksiin ja palautuksiin kuluvaa aikaa; se parantaa järjestelmien käytettävyyttä ja pienentää tältä osin kustannuksia. Ratkaisut helpottavat oleellisesti myös muutostilanteita, joissa tietojärjestelmien vaihtamisen tai yritysostojen yhteydessä joitakin järjestelmiä poistetaan käytöstä. Tiedon elinkaaren hallinnassa on myös huomioitava arkistonmuodostussuunnitelma, joka perustuu arkistolakiin (831/1994).

Marshall kumppaneineen (2015) on todennut, että informaatioteknologia on nopeasti kehittynyt niin, että tietoa voidaan esittää reaaliaikaisesti (myös Kaula 2015, 141). Jo nyt datan keräämistä ja sen analysointia hyödynnetään laajasti organisaation toimintaa koskevassa päätöksenteossa. Lisäksi Virtasen ja muiden (2015) mukaan verkostoituneessa ja avoimessa yhteiskunnassa ongelmana ei ole datan saatavuus. Kysymys on pikemmin datan analysoinnista ja sen tuottaman informaation käytöstä päätöksentekotilanteessa sekä olennaisen informaation hyödyntämisestä tietämyksen lähteenä.

Rajin (2013, 183–185) mukaan tarvittavan tiedon toimittaminen päätöksenteon tueksi juuri oikeaan aikaan korostuu nykyisessä liiketoiminta- ja IT-ympäristössä. Hänen mukaansa tiedon hyödyntäminen edellyttää historiatiedon, operatiivisen tiedon ja reaaliaikaisen tiedon tehokasta yhdistelemistä.

Brynjolfsson, Hitt ja Kim (2011) ovat omassa tutkimuksessaan päätyneet johtopäätökseen, että relevanttiin dataan perustuvan päätöksenteon (data driven decision making) ja organisaation suorituskyvyn välillä on suora syy-seuraussuhde (Soininen 2021). On siis perusteltua tarkastella, miten johto hyödyntää tietosuojatyön strategisessa johtamisessa toimintaympäristössä syntynyttä dataa, miten kyseinen data syntyy sekä miten datasta jalostetaan informaatiota laadukkaan tietosuojatyön toteuttamiseksi.

Tekniset, fyysiset sekä hallinnolliset tietoturvakontrollit nähdään entistä kriittisempänä strategisena voimavarana menestyvässä liiketoiminnassa, koska niiden avulla turvataan rekisteröidyn henkilötiedot. Tietoturvaa voidaan verifioida useilla eri standardeilla, ohjeilla sekä kriteeristöillä. Organisaatiossa tietojenkäsittelijöiden tulee olla tietoisia tietoturvapolitiikoista, joissa edellä mainitut standardit, ohjeet ja kriteeristöt on kuvattu, ja ideaalitilanteessa he ovat

sitoutuneet niihin (Siponen 2000). Tietosuojan ja tietoturvan välinen kytkös ja vuorovaikutus näyttääkin syntyvän siitä, että EU:n tietosuoja-asetuksessa kuvattuja henkilötietojen käsittelyn vaatimuksia toteutetaan aiemmin kuvattujen tietoturvastandardien, ohjeiden sekä kriteeristöjen avulla.

3 AIEMPI TUTKIMUS AIHEESTA

Yleisesti tietosuojaan liittyvien tutkimusten fokus on ollut sekä tietosuojatyön juridiikassa että teknisen tietoturvan yksityiskohtien arvioinnissa; aiheina ovat olleet esimerkiksi tietojenkäsittelyssä tapahtuvat virheet, tietojen toissijainen käyttö ja luvaton pääsy tietoihin. Viime aikoina tutkimusparadigmassa on tapahtunut muutos kohti yksityisyyden tarkastelua laajempana kokonaisuutena. Tarkat tutkimukset, jotka tuottavat näyttöön perustuvia prosesseja tai testaavat tietosuojassa esiintyviä syy-seuraussuhteita, toisivat suurta lisäarvoa. Niiniluoto peräänkuulutti jo vuonna 2011 tutkimuksia, jotka tarjoavat tulkintoja todellisen tilan tai käyttäytymisen muutoksista. Tämä eroaa asenteiden, uskomusten ja aikomusten tarkastelusta.

Tiedolla johtamista tietosuojatyössä pilvipalveluiden yhteydessä ei ole juurikaan tutkittu. Työn taustaksi haettiin vuosien 2018 ja 2023 väliseltä ajalta kansainvälisiä artikkeleita sekä ammattikirjallisuutta ensisijaisesti Jyväskylän yliopiston kirjaston hakukoneella Science & Technology -tietokannasta. Hakusanoina olivat tietosuoja, tietoturva, riskienhallinta, pilvipalvelut, EU tietosuoja-asetus, kansallinen tietosuojalaki ja tiedolla johtaminen (knowledge management). Haun tulos oli 320 artikkelia, joista osa ei sisällöllisesti vastannut haun tavoitteita. Kokeilin myös hakuyhdistelmiä ”EU tietosuoja-asetus + pilvipalvelut (GDPR + cloud services)” sekä ”tietosuoja + tiedolla johtaminen (GDPR + knowledge management)”, mutta se ei muuttanut haun tuloksia.

Aihepiirin tuoreus näkyy siinä, että olen päätynyt käyttämään tutkimukseni lähteinä poikkeuksellisen paljon korkeakoulujen pro gradu -tasoisia tutkielmia ja opinnäytteitä. Mielenkiinto aiheen akateemiseen tutkimiseen on ollut suurta nimenomaan korkeakouluopiskelijoiden keskuudessa, ja tutkielmia on tehty tehokkaasti nopealla aikataululla.

Myös tutkimuksia, joita voisi verrata suoraan käsillä olevaan tutkimukseen, on haettu. Tämän kirjallisuuskatsauksen rajaus ovat vuodet 2019–2022. EU:n tietosuoja-asetus astui voimaan vuonna 2016, ja sitä seurasi kahden vuoden siirtymäaika. Aiheeseen liittyvää tutkimusta alettiin julkaista erityisesti vuoden 2019 alusta.

Vertailtavaa tutkimusaineistoa haettiin eri tieteellisistä tietokannoista hakusanayhdistelmällä ”data privacy + public cloud” vuodesta 2019 alkaen, ja tuloksena oli noin 16 000 artikkelia. Tästä joukosta haettiin otsikon perusteella artikkeleita, jotka sisältävät viittauksia joko tietosuojajuridiikkaan, tietoturvaan, riskinarviointiin, sisään rakennettuun ja oletusarvoiseen tietosuojaan sekä hallinnolliseen ja operatiiviseen tietosuojaan. Kun tarkentavaksi hakusanaksi lisättiin ”knowledge management”, hakutulos kasvoi yli 17 000 artikkeliin, mutta samalla osuvuus heikkeni merkittävästi. Julkaisut, jotka ovat tämän tutkimuksen kanssa joiltain osin vertailukelpoisia, sisältävät mm. seuraavia avainkäsitteitä:

- risk management
- operatiivinen tai hallinnollinen tietosuoja
- data access control in the cloud computing
- confidentiality and integrity
- data storing in public cloud
- IoT data
- data encryption
- medical data
- electronic patient records and privacy
- blockchain
- access control
- masking methods
- outsourced data control
- privacy by design
- GDPR
- US law and privacy
- Schrems II
- data splitting
- anonymization.

Seuraavat julkaisut kuvaavat aiheen ympärillä käytävää diskurssia. Ne edustavat hyvin aiheeseen liittyviä julkaisuja, ja niiden tutkimusorientaatio on lähellä tätä tutkimusta.

Chadwick ym. (2020*)* lähestyvät tietosuojan poikkeamien ennaltaehkäisevää työtä lisäämällä kyberuhkatiedon analysointia, joka mahdollistaa kyberhyökkäysten paremman ennustamisen, ehkäisemisen ja lieventämisen. Tietosuojauhkien ennaltaehkäisyksi esitetään erilaisten anonymisointi- ja pseudonymisointimenetelmien hyödyntämistä sensitiivisten tietojen, esimerkiksi henkilötietojen, salaamisessa pilvipalveluissa. Kirjoittajat lähestyvät ilmiötä kyberturvallisuuden tarjoamien menetelmien viitekehyksestä, jossa korostetaan kaikkien toimijoiden yhteistyötä, ennustettavuutta, ehkäisemistä sekä mitigointia teknisin kontrollein. Artikkelissa esitellään pilvipohjaisen tiedonjakoinfrastruktuurin viisiportainen luottamusmalli, joka kuvaa arkaluonteisten ja luottamuksellisten tietojen jakamista tietoturvaan perustuvin ratkaisuin.

Artikkelissaan Wang ym. (2020) esitellyssä tutkimuksessa käytetään käsitettä liiketoiminta-analyysi. Sen voisi tulkita olevan lähellä tässä

väitöstutkimuksessa käytettyä tiedolla johtamisen käsitettä. Artikkelissa kuvataan, miten liiketoiminta-analytiikan mekanismi parantaa pilvipalvelujen tietoturvan hallintaa, pilvipalvelujen turvallisuutta. Tutkimuksen johtopäätökset tarjoavat yrityksille hyödyllisiä viitteitä siitä, miten ne voivat vahvistaa pilvipalvelujen tietoturvan hallintaa liiketoiminta-analytiikan avulla.

Artikkelissaan Ali ym. (2020) esittävät pilvipalvelujen tietoturvavaatimusmallia, jonka komponentit ovat tietoturva-, riskinarviointi-, lakisääteiset ja vaatimustenmukaisuusvaatimukset sekä liiketoimintavaatimukset ja tekniset vaatimukset. Näiden avulla julkishallinnon virastot voivat tarkastella pilvipalvelujen tietoturvaa tasapainoisesti. Mallin avulla organisaatiot voivat määritellä yhteisiä tietoturvavaatimuksia pilvipalveluiden käyttöönotolle.

Purnaye ja Kulkarni (2022) esittävät kattavan katsauksen pilvirikostekniikan tutkimussuuntauksesta. He ehdottavat pilvipalvelujen paradigmoihin perustuvaa pilvirikosteknistä taksonomiaa sekä pilvipohjaisia rikosteknisiä ratkaisustrategioita.

Tabrizchin ja Kuchaki Rafsanjanin (2020) katsauksessa kuvataan pilvipalvelujen tietoturvaongelmia ja -vaatimuksia, tunnistettuja uhkia ja tunnettuja haavoittuvuuksia. Työn tarkoituksena on analysoida pilvipalvelujen eri komponentteja sekä nykyisiä turvallisuus- ja yksityisyysongelmia, joita järjestelmät kohtaavat. Lisäksi työssä esitetään uusi luokitus turvallisuusratkaisuille. Artikkelissa tutkitaan yksityiskohtaisesti tietoturvahaasteita, joita pilvipalvelujen tarjoajat, tietojen omistajat sekä loppukäyttäjät kohtaavat.

Bruma (2020) tuo esille, että yksi keskeinen syy siihen, miksi organisaatiot välttävät siirtymistä julkiseen pilveen, on huoli strategisten tietojen menettämisestä. Tutkijat korostavat pilvipalvelun käyttöönoton alkuvaiheessa tehtävän riskinarvioinnin tärkeyttä. Tämä lisäksi he korostavat, että riskinarvioinnin pitää olla jatkuvaa. Se on kirjoittajien mukaan välttämätöntä tehtäessä strategisia päätöksiä turvamekanismeista. Artikkelissa esitellään tietoturvariskien arviointiprosessi ja esitetään tietoturvariskin määrittämisen mallia, joka antaa yleiskuvan haavoittuvuuksista sekä niiden vaikutuksista. Malli auttaa organisaatioita valitsemaan oikeat menetelmät optimaalisen tietoturvatason varmistamiseksi.

Yang ym. (2020) nostavat esille, miten mm. julkishallinto siirtää aktiivisesti tietojaan pilveen. Artikkelissa muistutetaan riskeistä, esimerkiksi luvattomasta pääsystä, tietovuodoista, arkaluontoisten tietojen paljastamisesta ja yksityisyyden rikkomisesta. Artikkelissa on kattava katsaus tietoturvaa ja yksityisyyttä käsittelevään kirjallisuuteen, tietojen salaustekniikkaan ja sovellettaviin vastatoimiin pilvitallennusjärjestelmässä (mm. tiedon luokittelu, arkkitehtuuri ja sovellukset). Tämän perusteella on tehty analyysi pilvitallennusjärjestelmän tietoturvan ja yksityisyyden suojan haasteista ja vaatimuksista.

Markopoulou ym. (2019) kuvaavat ensimmäistä EU:n tasolla annettua lainsäädäntöä, jolla suojataan verkko- ja tietojärjestelmiä EU:n alueella. Artikkelissa kuvataan ENISA:n roolia tämän direktiivin täytäntöönpanossa ja sen suhdetta EU:n yleiseen tietosuoja-asetukseen.

Chenthara ym. (2019) luovat kattavan katsauksen terveydenhuollon tietojärjestelmien tietoturvallisuuteen ja yksityisyydensuojan haasteisiin ja kuvataan

tapoja, joilla varmistetaan terveystietojen yksityisyys käytettäessä pilviteknologiaa. Artikkelissa korostetaan kyberturvallisuuteen liittyviä tutkimushaasteita ja -suuntia rakennettaessa elektronisten potilastietojärjestelmien tietoturvamalleja. Tutkimus nostaa esiin kriittisiä kysymyksiä terveydenhuollon tietojärjestelmien tietoturvasta ja yksityisyyden suojasta. Kirjoittajat muistuttavat, että suuret erityistä henkilötietoa sisältävät tietomassat muodostavat vakavia yksityisyyttä ja turvallisuutta koskevia haasteita, joiden huomioiminen on välttämätöntä. Jatkotutkimuksissa olisikin kirjoittajien mukaan keskityttävä tehokkaisiin ja kattaviin turvamekanismeihin sekä tutkittava myös tekniikoita, joilla pidetään yllä potilaiden tietojen eheyttä ja luottamuksellisuutta.

George (2022) nostaa esille pilvessä poikkeusoloissa tapahtuvan tietojen käsittelyn. Tarkoituksena on lisätä tietoisuutta Ukrainan ja Venäjän sodan vaikutuksista pilviteknologian käyttöön sekä siitä, miten poikkeusolot vaikuttavat, kun julkishallinnon organisaatiot ovat riippuvaisia kolmansilta mailta saamastaan tuesta. Artikkelissa muistutetaan oikeudellisista, sopimusperusteisista, taloudellisista sekä palvelujen laatuun ja yhteensopivuuteen, tietoturvaan ja tietosuojaan liittyvistä haasteista, joita poikkeusolot tuovat mukanaan.

Pilvipalvelujen kehityksen myötä yksityisyyden turvaan liittyvä keskustelu on yhä näkyvämpää. Sun (2020) tarkastelee tietosuojatutkimuksen edistymistä teknologisesta viitekehyksestä. Tutkimus esittelee muutamia yksityisyydensuojan turvallisuusriskejä pilvipalveluissa ja kuvaa yksityisyydensuojan kehitystä. Artikkeli esittelee useiden teknologioiden, kuten kulunvalvonnan salausteknologioiden, yhdistelemistä ongelman ratkaisemiseksi.

Gupta ym. (2023) ehdottavat suojattua tietosuojamenetelmää yksityisyyden säilyttämiseen pilviympäristössä. Tehokas osiointi, osittainen purkaminen ja analysoiminen varmistavat tiedon turvallisen tallennuksen ja jakamisen ja sen myötä pilvipalvelun turvallisuuden ja yksityisyyden.

Koronaviruspandemian aikana terveydenhuollon viranomaiset kehittivät kontaktien jäljityssovelluksia keinona jäljittää virusta ja hidastaa sen leviämistä. Sowmiya ym. (2021) analysoivat jäljityssovellusten turvallisuuteen ja yksityisyyteen liittyviä puheenvuoroja ja keskusteluja. Toimijoiden välillä näyttää olleen suuria näkemyseroja yksityisyydensuojasta ja pilviteknologiaan tukeutuvista massiivisista keskitetyistä tietovarannoista.

Sharma ym. (2020) nostavat esille, että pilvipalvelujen käyttöönotto on luonut organisaatioille lupauksia merkittävistä ICT-kustannussäästöistä. Kyberuhkien torjuntaan pilviympäristöissä on allokoitu resursseja, mutta silti pilvipalveluihin liittyy edelleen joukko vakavia ja monimutkaisia tietoturva- ja tietosuojahaasteita. Vaikka pilvipalvelujen tietoturvasta on keskusteltu laajalti ja kattavia ohjeita on laadittu, tietosuoja ei näytä pilvipalveluja käytettäessä olevan tietosuoja-asetuksen vaatimusten mukaista.

Artikkelissa esitellään systemaattinen katsaus aiempaan kirjallisuuteen, joka liittyy pilvipalvelujen tietosuojakysymyksiin, sekä korostetaan tarvetta luoda pilvipalveluihin yksityisyyden suojan kriteerit. Tutkimuksen yhteenvetona todetaan, että pilvipalveluiden tietosuoja on puutteellista. Artikkeli voi

kirjoittajien mukaan toimia oppaana yksityisyyden suojan rakentamisessa ja parantamisessa.

Liu ym. (2020) tuovat esille mahdollisuuden hyödyntää pilvipalveluiden tallennus- ja laskentaresursseja alustana koneoppimiselle. Samanaikaisesti tietosuoja on noussut kirjoittajien mukaan yleiseksi huolenaiheeksi pilviavusteisessa koneoppimisessa. Työssä tutkitaan, miten ns. päätöksentekopuun käyttöä voidaan tehokkaasti kouluttaa ja arvioida pilvessä ja samalla saavuttaa vaatimustenmukainen yksityisyydensuoja. Ehdotetussa ratkaisussa selkeytetään toimijoiden tietosuojaan liittyviä rooleja, vastuita ja velvollisuuksia koulutusprosessin suunnitteluvaiheessa hyödyntämällä menetelmänä päätöksentekopuuta. Yksityisyyden ja tehokkuuden välille luodaan yleisesti hyväksytty kompromissi, jota arvioidaan päätöspuun arviointijärjestelmällä.

Gozman ja Willcocks (2019) huomauttavat, että pilviteknologioiden laajamittainen käyttöönotto sekä palveluiden ulkoistaminen etenevät nopeasti, mutta pilvijärjestelyihin liittyvät haasteet ja riskit aiheuttavat huolta viranomaisten keskuudessa maailmanlaajuisesti. Artikkelissa keskitytään ymmärtämään pilvipalvelujen käyttöönottoon liittyviä erityisiä riskejä sekä käyttöön otettavia säännöksiä ja seuraamuksia sääntöjen noudattamatta jättämisestä etenkin finanssisektorilla. Tulosten perusteella artikkelin kirjoittajat ovat rakentaneet kehikon, joka auttaa päättäjiä arvioimaan vaatimustenmukaisuusriskejä, jotka vaikuttavat olennaisesti kriittisiin palveluihin.

Edellä esitellyissä julkaisuissa käsitellään hyvinkin syvällisesti yleensä vain yhtä tietosuojan hallintamallin osa-aluetta, usein teknistä tietoturvaa. Holistista tarkastelua, johon omassa tutkimuksessani pyrin, ei juurikaan ole. Ero tutkimukseeni näyttää olevan, mikä on julkaisujen kohderyhmä ja miten julkaisut tukevat organisaatioiden tietosuojan kypsyystason lisäämistä sekä mikä on tuotetun uuden tiedon vaikuttavuus tietosuojan holistisessa kehityksessä. Tiedolla johtamisen teorian hyödyntämistä valtionhallinnon tietosuojatyössä ei hakujen perusteella tullut esille. Oman tutkimukseni kontribuutiona voidaan pitää sitä, että työssä tuodaan esille henkilötietojen käsittelyssä esiintyviä potentiaalisia ristiriitoja, joita globaalien pilvipalveluiden käytössä on EU:n tietosuoja-asetuksen (GDPR) näkökulmasta. Valtorissa ja laajemminkin valtionhallinnossa eri päätöksentekoportaiden tulee kyetä reagoimaan ristiriitoihin, joita syntyy, kun globaalien pilvipalveluiden tarjoajat noudattavat sellaista lainsäädäntöä, joka arvottaa kansallisen turvallisuuden yksityisyydensuojan edelle (Pohjalainen 2018). Myös tietosuojatyön roolit, vastuut ja velvoitteet ovat edelleen toimijoille epäselvät. Euroopan unionin alueen yhteinen tietosuoja-asetus vaatii organisaatioiden johdolta entistä yksityiskohtaisempaa kokonaisturvallisuuteen liittyvää suunnittelua henkilötietojen käsittelyssä.

4 TUTKIMUSTA LÄPILEIKKAAVAT TEEMAT

4.1 Pilvipalvelut

Pilvipalveluista ei ole eksplisiittistä, selkeästi rajaavaa määritelmää. Sanastokeskus on määritellyt pilvipalvelut seuraavasti: ”hajautettu verkkopalvelu, jossa tietokoneita, ohjelmia ja tietoteknisiä palveluja käytetään verkon kautta” (Sanastokeskus 2019). Määrittelyä on tarkennettu, ja siihen on lisätty huomautus:

> Tietotekniikan resurssipalvelussa asiakas voi vuokrata lähes kaiken tarvitsemansa tietotekniikan verkon kautta. Tällöin asiakkaan ei tarvitse ostaa esimerkiksi palvelimia, suurta laskentatehoa tarjoavia tietokoneita tai ohjelmia omakseen, vaan hän voi käyttää niitä tarpeen mukaan verkkoyhteyden kautta. Tietotekniikan resurssipalvelu voi olla myös organisaation sisäinen palvelu, jota sen työntekijät voivat käyttää maailmanlaajuisesti. (Sanastokeskus 2019.)

Pilvi-sana otettiin tietojenkäsittelyn käyttöön 1980-luvulla teleoperaattoreiden alkaessa merkitä verkkojaan pilvisymbolilla (Heino 2010, 32–33). John McCarthy (1961) esitteli tietokonekapasiteetin jakamista samoilla periaatteilla kuin sähköä tai vettä. Pilvitoimintamallin kehitys otti merkittävän harppauksen 2000-luvun alussa Amazonin alkaessa tarjota ulkoisille tahoille ylimääräistä palvelinkapasiteettia. Vuotta 2002 pidetään virstanpylväänä, sillä silloin käynnistyi Amazonin Web Services -palvelu. (Heino 2010, 33–34.)

Yksinkertaisimmillaan pilvipalvelut ovat tietoverkkojen välityksellä käytettäviä ohjelmisto- tai kapasiteettipalveluja. Näistä ehkä tunnetuin on Googlen tarjoama ilmainen Google Apps -työvälineohjelmisto, joka sisältää mm. sähköpostin, kalenterin sekä taulukkolaskenta- ja tekstinkäsittelyohjelman. Palvelun käyttöarvo kuluttajalle on siinä, että tarjottujen sovellusten käyttöön tarvitaan ainoastaan verkkoselain, mikä tuo merkittäviä säästöjä ohjelmisto- ja kapasiteettikustannuksiin (Salmio 2012).

Pilvipalveluiden merkityksellisen kaupallistumisen voidaan katsoa alkaneen, kun yritykset alkoivat ulkoistaa omia palvelinresurssejaan, tietokantojaan

sekä sovelluksiaan. Tällä hetkellä suurimmat pilvipalveluita tarjoavat yritykset ovat Amazon, Google, Microsoft, Salesforce, IBM sekä Alibaba Cloud.

Pilvipalvelujen käyttäjien määrä on eksponentiaalisessa kasvussa, ja julkishallinnon tietohallintostrategiat näyttävät seuraavan tätä trendiä. Pilvipalveluiden määrittely on osoittautunut kuitenkin hyvin kirjavaksi; palveluiden tulisi vähintään sisältää National Institute of Standards and Technologyn (NIST) määrittelemiä ominaisuuksia, jotta niiden voidaan katsoa olevan pilvipalveluja.

Käytön kannalta pilvipalvelussa ei ole merkityksellistä, millä teknisillä ratkaisuilla se on toteutettu. Ominaista palveluille on, ettei käyttäjillä välttämättä ole tietoa, missä itse palvelimet sijaitsevat tai mitkä ovat niiden toiminnalliset funktiot. Pilvipalveluiden perusperiaatteisiin kuuluu, että nämä kokonaisuudet ovat palveluntarjoajan vastuulla. Viranomaistoiminnan luonteen vuoksi rekisterinpitäjien tulee kuitenkin tietää ja ymmärtää yksityiskohtia palvelun toteutuksesta, kuten missä tietoja säilytetään, miten tietoa hallitaan sen elinkaaren aikana ja millainen on tietojen exit-strategia (Salmio 2012).

NIST on määritellyt pilvitoimintamallin, sen ominaisuudet, palvelumallit sekä pilvimallit. Kyseiset mallit koostuvat kahdeksasta yleisestä ominaisuudesta: skaalautuvuus, yhtenäisyys, virtualisointi, joustava tietojenkäsittely, halvat ohjelmistot, maantieteellinen jaettavuus, palvelusuuntautuneisuus ja kehittyneet turvateknologiat. (Mell & Grance 2009, 14.)

Pilvimallit ovat seuraavat: yksityispilvi, yhteisöpilvi, julkinen pilvi sekä hybridipilvi. Palvelumalleja on kolme: ohjelmisto palveluna (SaaS, software as a service), alusta palveluna (PaaS, platform as a service) sekä infrastruktuuri palveluna (IaaS, infrastructure as a service). (Mell & Grance 2009, 11–13.)

Ohjelmisto palveluna (SaaS, software as a service) -palvelumallin periaatteena on, että palveluntarjoajat tarjoavat asiakkaille sovelluksia palvelimiltaan tietoverkkojen välityksellä. Keskeistä tässä palvelumallissa on, että vastuu palveluiden ylläpidosta, päivityksistä, käyttäjätuesta sekä tietoturvasta on palvelun tarjoajalla. SaaS-palveluja markkinoidaan kustannustehokkaina ja joustavina ratkaisuina. (Pervez ym. 2010.)

Alusta palveluna (PaaS, platform as a service) -palvelumalli keskittyy tarjoamaan sovelluskehitysalustoja ja kehitystyökaluja tietoverkkojen välityksellä niin, että palveluntarjoajan vastuulla on kehitys- ja testiympäristö. Infrastruktuuri palveluna (IaaS, infrastructure as a service) -palvelumalli tarjoaa käyttäjilleen virtualisoituja laitteistoja sekä mm. tallennustilaa. Käyttäjät voivat itsenäisesti kontrolloida virtuaalisiin laitteistoihin haluamansa käyttöjärjestelmät ja sovellukset, mutta itse pilvi-infrastruktuuria kontrolloi palveluntarjoaja. (Salmio 2012.)

Pilvipalvelut jaetaan pilvimalleihin sen perusteella, ketkä palveluja kontrolloivat ja käyttävät. NIST:n määrittelemä yksityispilvimalli on suljettu verkkopalvelu, jonka kohderyhmänä ovat ainoastaan toimijan määrittelemät sidosryhmät. Yhteisöpilvi on käsitteenä hieman laajempi. Tällöin pilvi-infrastruktuuri on jaettu useiden yritysten kesken, joilla on esimerkiksi yhteisiä tehtäviä. Toimijat voivat halutessaan itse kontrolloida palveluja. Julkisen pilvi-infrastruktuurin periaate on, että se on kaikkien saatavilla ja sitä kontrolloi vain ja ainoastaan

palveluntarjoaja itse. Hybridipilvi määritellään useamman pilvimallin yhdistelmäksi. (Nodehi ym. 2013.)

4.1.1 Pilvipalveluita tarjoavat yritykset

Suurimmat ja tunnetuimmat palveluntarjoajat ovat Amazon, Google, IBM sekä Microsoft. Amazon tunnetaan pisimpään markkinoilla toimineena pilvipalveluiden tarjoajana; se on tarjonnut Amazon Web Services (AWS) -verkkopalvelujaan jo vuodesta 2006 alkaen. Amazon Web Services on keskittynyt pääasiassa infrastruktuuripalveluihin (IaaS), ja sitä käytetään maailmanlaajuisesti. (Paajanen 2017.) Amazon Elastic Compute Cloudin (Amazon EC2) perusajatus on tarjota käyttäjilleen tehokkaita virtuaalisia laitteistoja, instansseja. Ratkaisu tarjoaa mahdollisuuden käyttää omia sovelluksia tehokkaassa virtuaaliympäristössä edullisesti. (Paajanen 2017.) AWS:n lisäarvon kilpailussa koetaan syntyvän instanssien skaalautuvuudesta sekä hinnoittelusta (Salmio 2012).

Google tarjoaa SaaS-palveluja Google Apps -ohjelmiston muodossa sekä PaaS-palveluja Google App Enginen (GAE) avulla. Google Apps sisältää monia sovelluksia kalenterista sähköpostiin, kun taas Google App Engine on sovelluskehitysalusta. (Hashem ym. 2015.)

Myös IBM tarjoaa nykyisin pilvipalveluita, ja kaikki kolme palvelumallia ovat edustettuina. IBM:n pilvipalvelut ovat seuraavat: IBM LotusLive (SaaS), IBM LotusLive iNotes (SaaS), CRS Informaation suojauspalvelut (US) (SaaS), IBM Smart Business Test Cloud (US) (PaaS), IBM Smart Business Storage Cloud (IaaS) ja IBM Cloud Computing -työasemapalvelut (IaaS). (IBM 2012.)

Microsoft mainostaa tarjoavansa yrityksille sekä yksityisille käyttäjille monipuolisia pilvipalveluratkaisuja edullisesti. Tunnetuimmaksi Microsoftin pilvipalveluksi on noussut vuonna 2010 julkaistu Windows Azure sekä myöhemmin samana vuonna julkistettu Office 365. SaaS-palveluihin kuuluva Office 365 on käytännössä pilvessä käytettävä Microsoft Office, joka sisältää ohjelmia tekstinkäsittelystä kalenteriin. Käyttäjät pääsevät tiedostoihinsa käsiksi mistä tahansa vaivattomasti. (Katzer & Crawford 2013.) Windows Azure on sovellusalustapalvelu, jolla käyttäjät voivat kehittää, testata ja käyttää sovelluksiaan. Windows Server Hyper-V on IaaS-palveluihin kuuluva virtualisointialusta, joka mahdollistaa tehokkaat virtualisoidut työasema- sekä palvelinympäristöt. (Salmio 2012.)

4.1.2 EU:n tietosuoja-asetuksen ja pilvipalveluiden suhde

Yksityisyyssääntely on Yhdysvalloissa hajanaisen lainsäädännön vuoksi varsin monimutkaista, ja se tarjoaa mahdollisuuden lavealle henkilötietojen käsittelylle. Yhdysvalloista kerätty data osoittaa, että yksilöivän tiedon yhdistämisessä ja analysoinnissa on pitkään ja massiivisesti käytetty hyväksi valvontaa, salakuuntelua sekä erilaisia turvallisuustekniikoita. Tämän perusteella onkin ymmärrettävissä, miksi yhdysvaltalaisille toimittajille näyttää olevan haasteellista osoittaa, että heidän palvelunsa täyttävät EU:n tietosuoja-asetuksen vaatimukset. Euroopassa taas yleinen tietosuoja-asetus pyrkii tarjoamaan kattavan kehyksen, jota tukee ihmisoikeuslaki. Digitaalisen kehityksen näkökulmasta näyttääkin siltä,

että Euroopan unioni pyrkii globaaliksi ”tietosuojavaltuutetuksi”. (Anderson 2020, 821–833.)

EU:n tietosuoja-asetuksen mukaan pilvipalveluiden käyttöönotossa on varmistuttava siitä, että henkilötietojen käsittelyn kokonaisvastuu on rekisterinpitäjällä. Rekisterinpitäjän tulee tehdä vaikutusten- ja riskinarviointi, jonka perusteella se hyväksyy niin sanotut jäännösriskit. Rekisterinpitäjä ja tietojenkäsittelijä sopivat yhteisesti tietojenkäsittelyn periaatteista. Tietojenkäsittelijältä tulee löytyä näyttöä siitä, että tietoja käsitellään asiaankuuluvalla tavalla. Tarkasteltaessa riskejä ylätasolla tulee varmistua siitä, että pilvipalvelut ovat ominaisuuksiltaan rekisterinpitäjän vaatimusten mukaisia kaikilta osin. Lisäksi tulee arvioida tiedon elinkaaren hallinta, exit-strategia (miten tiedot siirretään järjestelmästä toiseen), palvelun saavutettavuuteen ja käytettävyyteen liittyvät riskit sekä toimittajariippuvuuteen liittyvät riskit. Pilvipalveluihin on syytä ennen käyttöönottoa kohdistaa kolmannen osapuolen suorittama tietoturvallisuuden arviointilain mukainen menettely ja tietosuojan ja -turvan vaikutusten arviointi, joilla täytetään osoitusvelvollisuus.

Osoitusvelvollisuus on keskeinen periaate tietosuoja-asetuksessa, ja sen tarkoituksena on näyttää, miten rekisterinpitäjä kunnioittaa rekisteröityjen oikeuksia. Konkreettisesti tämä tarkoittaa, että rekisterinpitäjän on kyettävä osoittamaan noudattavansa tietosuojalainsäädäntöä. Esimerkiksi poikkeamatilanteissa voidaan osoitusvelvollisuuden avulla todentaa, miten aktiivisesti on pyritty tunnistamaan tietosuojaan liittyviä riskejä.

Rekisterinpitäjän on vaadittava sekä itseltään että kaikilta tietojenkäsittelijöiltä näyttöä siitä, että käytössä olevat tekniset ja organisatoriset toimenpiteet täyttävät osoitusvelvollisuuden vaatimukset. Toimenpiteitä ovat mm. artiklan 30 mukainen henkilötietojen käsittelyn yleinen kuvaus, artiklan 25 mukainen kuvaus sisäänrakennetun tietosuojan periaatteiden toteutumisesta omassa toiminnassa, artiklan 24 mukainen toimintaperiaatteiden kuvaus, artikloiden 6–10 mukainen käsittelyn oikeusperustan kuvaus sekä artiklan 35 mukaiset vaikutustenarvioinnit ja ennakkokuulemista koskeva dokumentaatio. (Korpisaari ym. 2018.)

Tutkimuslaitos Gartner on tehnyt vuoden 2010 alussa tutkimuksen yleisimmistä pilvipalveluiden käyttöönottoon liittyvistä huolenaiheista. Tutkimuksen mukaan ylivoimaisesti suurin huolenaihe on palvelujen turvallisuus. Seuraavaksi suurin on huoli siitä, missä tallennettu data todellisuudessa sijaitsee, pääseekö siihen varmasti aina käsiksi ja onko tieto varmasti salassa.

Yleiseksi huoleksi on noussut pilvipalvelujen kontrolloimisen vaikeus. Huoli näyttää perustellulta siinä valossa, että palveluntarjoaja ylläpitää ja hallitsee palveluja. Tilanne on johtanut ns. ”vendor lock-in-tilanteeseen”, joka on suomeksi ”toimittajaloukku”: palveluntarjoajan vaihtamiseen liittyvä tietojen siirtäminen ja poistaminen on käytännössä mahdotonta ja vaihtokustannukset ovat niin suuret, että ne estävät palveluntarjoajan vaihtamisen.

Cloud Security Alliance (CSA) on listannut seitsemän suurinta pilvipalveluiden tietoturvauhkaa: palvelujen rikollinen ja luvaton käyttö, suojaamattomat rajapinnat ja API:t (application programming interface), epäluotettava sisäpiiri,

jaetun teknologian ongelmat, datan häviäminen ja vuotaminen, käyttäjätilien ja palveluiden kaappaaminen sekä tunnistamattomat riskit (Salmio 2012). Näistä kaikkien voidaan arvioida olevan kriittisiä uhkia myös henkilötietojen käsittelyssä.

Julkishallinnossa pilvipalveluiden hyödyntämisen lähtökohta on riskiperusteisuus, jota käytännössä toteutetaan aiemmin kuvatuilla tietoturvakontrolleilla. Lisäksi toiminnan arvioinnissa tulee huomioida hyötyjä, kuten skaalautuvuus, käytettävyys sekä kustannustehokkuus. (Lehto & Neittaanmäki 2014; Valtiovarainministeriö 2016.)

Yhdysvalloissa henkilötietojen luovuttamista kolmansille osapuolille ei ole rajoitettu niin tiukasti kuin EU-alueella. Tämä johtaa väistämättä ajatukseen, että EU:n tietosuoja-asetuksen näkökulmasta rekisteröidyn oikeudet saattavat olla uhattuna. (Van den Berg 2019.) Kun organisaatiot käyttävät yhdysvaltalaisten yritysten tarjoamia pilvipalveluita, myös osa palvelimista sijaitsee Yhdysvalloissa. Se tarkoittaa, että pilvipalveluissa käytettyjä henkilötietoja, joita on esimerkiksi yrityksen asiakasrekisterissä tai HR-järjestelmissä, suurella todennäköisyydellä siirtyy Yhdysvaltoihin.

Foreign Intelligence Surveillance Act (FISA) on Yhdysvalloissa vuonna 1978 hyväksytty laki, joka sääntelee Yhdysvaltain hallituksen tiedustelutoimintaa ulkomaiden kansalaisten ja ulkomaisten organisaatioiden suhteen. FISA määrittelee periaatteet, joita Yhdysvaltain tiedustelupalvelut ja lainvalvontaviranomaiset sitoutuvat noudattamaan kerätessään tietoa mm. Euroopan unionin alueelta. Periaate on, että Yhdysvaltain hallitus hakee tuomioistuimen hyväksynnän, ennen kuin se voi kerätä omaan käyttöönsä tietoja ulkomaalaisesta henkilöstä tai organisaatiosta, jonka epäillään olevan uhka Yhdysvalloille. Poikkeuksena tähän periaatteeseen on rikosepäilyt liittyen kansalliseen turvallisuuteen tai vakaviin rikoksiin, kuten esimerkiksi vakoiluun, terrorismiin tai kyberrikollisuuteen viittaava toiminta, jolloin Yhdysvaltain viranomaisilla on pääsy tietoihin ilman erillisitä lupaa (Ryan-Mosley 2023).

FISA on ollut viime vuosien aikana useiden muutosten kohteena, joiden tavoitteena on ollut antaa Yhdysvaltain hallitukselle enemmän valtaa valvoa ulkomailla toimivia viestintäyhtiöitä vakavien rikosten torjumista varten.

Toiminnan läpinäkyvyyden puute on nostanut huolta EU:n alueella, jossa kyseistä lainsäädäntöä on arvosteltu siitä, että se antaa Yhdysvaltain hallitukselle liikaa valtaa valvoa ulkomaalaisia ilman asianmukaista tuomioistuimen valvontaa ja että se rikkoo ihmisoikeuksia. Pilvipalveluissa tapahtuvan henkilötietojen siirron EU- ja ETA-alueiden ulkopuolelle nähdäänkin tämän valossa olevan vahvasti ristiriidassa EU:n rekisteröityjen oikeuksien kanssa.

Henkilötietojen siirto EU:n ja Yhdysvaltojen välillä on aiemmin tapahtunut eri toimijoiden välisen Privacy Shield -sopimuksen turvin. Sopimuksen tavoitteena oli luoda rekisteröidyn henkilötiedoille korkeatasoinen suoja. EU:sta Yhdysvaltoihin siirtyvien henkilötietojen käsittelyssä täytyi noudattaa lukuisia tietosuojasäännöksiä ja suojatoimia. Yhdysvaltojen lait eivät yleisesti, muutamia poikkeuksia lukuun ottamatta, oikeuta rekisteröityä saamaan hänestä kerättyjä henkilötietoja tai vaatimaan näiden tietojen oikaisua tai poistoa. Euroopan

komission mukaan EU oli saanut kirjalliset takeet Yhdysvalloilta siitä, ettei Yhdysvaltojen viranomaisilla tai tiedustelupalvelulla ole pääsyä henkilötietoihin ja että turvallisuusintresseihin perustuva tiedonkäyttö on selkeästi rajattu.

Yhdysvalloissa ei kuitenkaan ole yksityisyyttä koskevaa kansallista lakia, jolla kontrolloitaisiin henkilötietojen keräämistä ja käyttöä, vaan toimintaa ohjaavat useat osavaltiokohtaiset lait ja asetukset, jotka ovat ajoittain jopa keskenään ristiriitaisia. Tämän lisäksi valtion virastoilla ja teollisuudella on käytössään erilaisia ohjeistuksia (white paper), joita tulkitaan de facto -standardeina. Niitä pidetään yleisesti hyväksyttyinä parhaina käytänteinä, eikä niillä ole lain voimaa.

Edellä mainittujen asetusten ja ohjeistusten fokus on tietoturvan, yksityisten tiedostojen, asiakirjojen ja yleisesti datan suojelussa, mutta yksityisyys ja yksilön oikeudet on jätetty huomiotta. Sen sijaan yhdysvaltalainen lähestyminen henkilötietojen käsittelyyn on enemmänkin toimialasidonnaista (sector-spesific). Esimerkkejä mainitusta toimintamallista ovat The Health Insurance Portability and Accountability Act (HIPAA), joka sääntelee potilastietojen käsittelyä, Gramm-Leach-Bliley Act (GLBA) ja The Financial Services, jotka sääntelevät taloustietojen käsittelyä, sekä Telephone Consumer Protection Act (TCPA) ja Telemarketing Sales Rule, jotka ohjaavat tietojenkäsittelyä markkinoinnissa. (Pohjalainen 2018.) Lähimpänä EU:n tietosuoja-asetusta on Kalifornian kuluttajien yksityisyyttä koskeva laki (CCPA).

EU-tuomioistuin alkoi kiinnittää huomiota henkilötietojen käsittelyprosesseissa potentiaaliseen uhkaan, jossa EU-kansalaisten henkilötiedot siirtyvät tietojärjestelmistä ilman perusteita EU-alueen ulkopuolelle. Tuomioistuimen tulkinnaksi muodostui, ettei Privacy Shield -järjestely estänyt henkilötietojen perusteetonta käsittelyä. Tilanne johti Privacy Shield -järjestelyn kumoamiseen 16.7.2020 ilman siirtymäaikaa.

Euroopan tietosuojaneuvosto julkaisi 23.7.2020 lisäohjeistusta, ja tulkinta dokumentin pohjalta on, että komission hyväksymät vakiolausekkeet (standard contractual clauses, SCC) ovat edelleen pätevä suojamekanismi, kun tietoja siirretään EU- ja ETA-alueiden ulkopuolelle, mutta Yhdysvaltojen kohdalla tarvitaan myös lisäsuojakeinoja (supplementary measures). Soveltuvien lisäkeinojen pohtiminen ja vakiolausekkeiden riittävyyden arviointi ovat sekä rekisterinpitäjän että tietojenkäsittelijän velvollisuus. Tietojen pääkäsittelijän vastuulla on varmistaa, että tietojen alikäsittelijät täyttävät tietojenkäsittelylle asetetut vaatimukset, joihin keskeisesti liittyy henkilötietojen maantieteellisen sijainnin määrittely ja sen varmentaminen, etteivät kyseiset tiedot siirry määritettyjen maantieteellisten lokaatioiden ulkopuolelle.

Cloud Act on lyhenne, joka tarkoittaa Yhdysvaltain lainsäädännön Clarifying Lawful Overseas Use of Data -lakia, joka hyväksyttiin vuonna 2018. Laki laajentaa Yhdysvaltojen viranomaisten lainkäyttövaltaa siten, että se voi vaatia sähköpostien, dokumenttien ja muiden sähköisten tietojen luovuttamista Yhdysvaltain viranomaisille, vaikka ne sijaitsevat fyysisesti toisessa maassa. Laki merkitsee sitä, että Yhdysvaltain eri viranomaiset voivat pyytää digitaalista tietoa yhdysvaltalaisilta yrityksiltä myös silloin, kun tiedot on tallennettu maan rajojen ulkopuolelle, antamalla Yhdysvaltain hallitukselle mahdollisuuden solmia

sopimuksia muiden maiden kanssa, jotta tietojen luovutus olisi helpompaa ja nopeampaa. (Christakis 2019.)

Lain taustalla on oikeustapaus vuodelta 2013. Yhdysvaltain hallinto halusi Microsoftilta tietoja yksittäisestä käyttäjästä vakavaan rikokseen liittyvässä tapauksessa. Microsoft kieltäytyi luovuttamasta tietoja perustellen, että ne oli tallennettu Irlannissa sijaitsevaan palvelimeen ja näin ollen tietoa tulisi käsitellä EU:n lakien ohjaamana. Yhdysvaltojen mielestä Microsoftin oli yhdysvaltalaisena yrityksenä noudatettava Yhdysvaltain lakeja, vaikka tässä tapauksessa tiedot sijaitsivatkin toisessa maassa. Asiasta kiisteltiin vuosia eri tuomioistuimissa, minkä jälkeen Yhdysvaltain hallitus laati Cloud Actin, joka antoi Yhdysvaltain viranomaisille laillisen oikeuden vaatia pyydettyjä tietoja yhdysvaltalaisilta yrityksiltä (Daskal 2018, 71).

Koska EU:ssa tapahtuva henkilötietojen käsittely voi olla Cloud Act -lain ulottuvilla, vaikka EU:n yksiköt sijaitsisivat Yhdysvaltojen ulkopuolella, on Cloud Act saanut laajaa ja voimakasta kritiikkiä siitä, että se heikentää ihmisten yksityisyydensuojaa ja lisää Yhdysvaltain hallituksen valtaa. Kriitikot ovat huolissaan siitä, että tietojen luovutus Yhdysvaltain viranomaisille saattaa johtaa siihen, että henkilöiden tietoja käytetään väärin tai että Yhdysvaltain hallitus käyttää valtaansa väärin. (Barati ym. 2021.)

Henkilötiedot, jotka on tallennettu yhdysvaltalaisen pilvipalvelun tarjoamaan ympäristöön EU:n rajojen sisäpuolella, kuuluvat Cloud Actin piiriin. Edellä mainitut lait tarjoavat juridisen mahdollisuuden Yhdysvaltain viranomaisille pyytää tietoja, vaikka EU:n tietosuoja-asetuksen perusteella tietojen voidaan olettaa kuuluvan jäsenmaiden lakien suojan piiriin. Merkille pantavaa on, että vaikka Cloud Act antaa viranomaisille oikeuden pyytää tietoja, vaatimuksena on yhä, että Yhdysvalloilla on sopimus sen maan kanssa, josta tietojen luovuttamista pyydetään. Useat tietosuojatoimijat EU:n alueella ovat tuoneet esiin EU:n tietosuoja-asetuksen ja yhdysvaltalaisen lainsäädännön ristiriidan, joka tarjoaa mahdollisuuden luovuttaa henkilötietoja ilman sen suurempaa valvontaa. (Wachter & Mittelstadt 2019.)

4.1.3 Jaettu tietoturvan vastuumalli

Pilvipalvelussa vastuu tietoturvasta on jaettu rekisterinpitäjän (asiakkaan) ja tietojenkäsittelijän (palveluntuottajan) välillä. Pilvipalvelun valinnan alkuvaiheessa tietoturvakysymystä voidaan lähestyä mm. ennakoivan tietosuojan mallintamisen kautta. Se on osa suurempaa kokonaisuutta, joka huomioi tietosuojan ja tietoturvan välisen vuorovaikutuksen. Ennakoivan mallintamisen avulla rekisterinpitäjän vastuut ja velvoitteet tunnistetaan ennen palvelun käyttöönottoa. Tietoturvallisuuden vastuut ja velvoitteet tulee käsitellä palvelukohtaisesti.

Mikäli käyttöön otettavassa pilvipalvelussa käsitellään henkilötietoja, näille tiedoille tulee määritellä ja dokumentoida rekisterinpitäjä. Lisäksi on varmistettava, että rekisterinpitäjä tuntee vastuunsa ja velvoitteensa. Rekisterinpitäjän on luokiteltava palvelussa käsiteltävät henkilötiedot. Rekisterinpitäjä ja tietojenkäsittelijä sopivat yhteisesti tietoturvan arvioinnissa käytettävästä arviointikriteeristöstä. Tietosuojan vaatimuksenmukaisuuden määrittelyssä ja arvioinnissa

käytetään EU:n yleistä tietosuoja-asetusta (2016/679) ja kansallista tietosuojalakia (1050/2018) rinnakkain. Saatuaan päätöksentekoon tarvittavan informaation rekisterinpitäjällä tulee olla käsitys riskiarvion lopputuloksesta ja niin sanotusta jäännösriskistä. Tämä perustuu palvelun tietoturvallisuuden todentamiseen. Koska vastuu tietoturvasta on rekisterinpidosta vastaavan organisaation johdolla, sen tulee hyväksyä tai hylätä jäännösriskit. Mikäli päädytään hyväksymään jäännösriskit, tulee olla tiedossa, miten niitä hallitaan sekä miten jatkuva seuranta toteutetaan.

Tietojenkäsittelijän velvollisuutena on pystyä osoittamaan järjestelmien ja palveluiden vaatimustenmukaisuus. Tietojenkäsittelijän tulee informoida rekisterinpitäjää mahdollisista alihankkijoista (henkilötietojen alikäsittelijät), joilla on samat velvollisuudet kuin tietojen pääkäsittelijällä. Tietojenkäsittelijän tulee olla tietoinen siitä, että hän vastaa henkilötietojen alikäsittelijöiden tietoturvallisuudesta sekä toimintaprosesseista poikkeamatilanteissa. Tietojenkäsittelijä toteuttaa tietoturvallisuuden todentamisprosessin, jonka perusteella syntyy luotettava näyttö.

Haastavana toimittajien esittämien vastuunjakomallien käyttöönotossa on pidetty sitä, ettei henkilötietojen käsittely-ympäristöissä määritellä tarkemmalla tasolla henkilötietosisältöä. Tämän lisäksi haasteeksi nousevat henkilötiedon käsitteiden ja luokittelun erot (ks. alaluku 2.2.1).

4.2 Tiedolla johtaminen

Japanilaisten Ikujirō Nonakan ja Hirotaka Takeuchin esittämä tiedolla johtamisen teoria perustuu ajatukseen tietämyksen luomisesta (Nonaka & Takeuchi 1995). Prosessissa organisaatioissa luodaan uutta tietoa ja tietämyksen jakaminen tapahtuu vuorovaikutuksen kautta.

Nonaka ja Takeuchi erottavat eksplisiittisen ja hiljaisen tiedon. Eksplisiittinen tieto on ilmaistavissa sanoiksi, kun taas hiljainen tieto on henkilökohtaista tietoa, jota on vaikeampi ilmaista sanoin. Tiedolla johtamisen yksi keskeinen tavoite on muuntaa hiljainen tieto eksplisiittiseksi ja jakaa sitä organisaatiossa.

Tiedolla johtamisen teoria on adaptoitu yhdeksi johtamisen lähestymistavaksi, jossa päätöksiä tehdään käyttämällä tietoa ja analytiikkaa. Tiedolla johtamisen avulla päätöksentekijät saavat näyttöön perustuvaa tilannekuvaa organisaation toiminnasta ja sen kehitystarpeista. Nonaka ja Takeuchi (1995) korostavat tiedon ja tietämyksen merkitystä organisaatioissa ja esittävät, että organisaatioiden menestyminen perustuu kykyyn luoda, jakaa ja hyödyntää tietoa tehokkaasti. Lähestymistapa korostaa kulttuurin merkitystä tiedolla johtamisessa, joten organisaatioiden tulee olla valmiita muokkaamaan omaa kulttuuriaan ja prosessejaan, jotta ne voivat hyödyntää tiedolla johtamista tehokkaasti.

Taustalla on ajatus siitä, että päätöksiä ei pidä tehdä pelkästään kokemusten perusteella. Kokemuksissa vaikuttaa intuitiivinen ja tiedostamaton tiedonkäsittely, eikä intuitio ole aina luotettava lähde päätöksenteossa. Päätöksenteon tulee muodostua näyttöön perustuvan tiedon ja jaetun kokemuksen

vuorovaikutuksen summana. Bali ym. (2009) korostavat tiedolla johtamisessa myös tiedon visualisointia ja kommunikointia, jotka lisäävät datan ymmärrettävyyttä.

Tiedolla johtamisen teoriassa lähdetään ajatuksesta, että organisaatiot voivat hyötyä datan käytöstä monin tavoin. Yleisesti tiedolla johtamista hyödynnetään trendien tunnistamisessa ja tulevaisuustutkimuksessa, prosessien ja resurssien optimoinnissa, päätöksenteossa sekä uusien liiketoimintamallien kehittämisessä (Soininen 2021). Tiedolla johtamisen avulla toteutettavalla ennakointiin perustuvalla riskienhallinnalla autetaan organisaatioita myös tunnistamaan heikkoja signaaleja organisaatiossa tapahtuvasta ei-toivotusta toiminnasta. Teorian soveltaminen edellyttää organisaation kulttuurin ja prosessien muokkaamista siten, että datan kerääminen ja analysointi on jatkuvaa. Tämä auttaa organisaatioita saavuttamaan parempia tuloksia ja antaa kilpailuetua, koska päätöksentekijät voivat tehdä parempia ja perustellumpia päätöksiä (Jalonen 2015). Tämä vaatii investointeja teknologiaan, koulutukseen ja henkilöstön resursseihin. On tärkeää, että organisaatio pystyy hyödyntämään kerättyä tietoa ja saamaan siitä irti mahdollisimman suuren hyödyn.

Tiedolla johtamisen tarkoitus on tukea organisaatioiden toimintaa varmistamalla, ettei johtaminen perustu oletuksiin tai mielipiteisiin vaan näyttöön perustuvaan tietoon. Pelkkä data ei riitä päätöksenteon pohjaksi eikä lisäarvon tuottamiseen, vaan niihin tarvitaan datan perusteella tuotettua informaatiota. (Koraeus 2008.)

Tiedolla johtaminen mielletään usein erilaisten raporttien tarkasteluksi, joka kuitenkin on vasta tiedolla johtamisen lähtöpiste. Raportti sisältää kerättyä dataa ja asiantuntijan vastuulla on muodostaa datasta informaatiota tiedon pohjaksi, josta viisaus aikanaan muodostuu, mahdollistaen vision tulevaisuudesta. (Ahonen 2020.)

Yleispätevästä tieto-käsitteen määrittelystä on kiistelty kautta aikojen. Filosofit, kunnioittaen Platonin klassista tiedon määritelmää, ovat kuitenkin yksimielisiä muutamista tietoa koskevista vaatimuksista: sen tulisi olla objektiivista, tiedeyhteisön validoimaa ja kenen tahansa asiaan perehtyneen hyväksyttävissä olevaa, eikä sen tulisi perustua vain intuitioon. (Laaksovirta 1983.)

Termille ”knowledge management” on lukuisia erilaisia suomenkielisiä vastineita. Käsitteisiin ”knowledge” ja ”management” viitataan sekä erikseen että yhdistettynä useissa eri käsitefilosofioissa (Nonaka & Takeuchi 1995). Sanalla ”knowledge” voidaan tarkoittaa mm. tietoa, tietoja, tietämystä, kokemusta, tuntemusta ja taitoa. ”Management” on puolestaan käännetty mm. termeiksi käsittely, hoito, hallinto, johto, viisaus, taitavuus, viisas menettely ja tarkka huolenpito.

Yhdistettynä käsite on muotoutunut suomen kielessä tiedon ja tietämyksen hallinnaksi, osaamisen johtamiseksi sekä tietojohtamiseksi (Kivinen 2008). Kun knowledge managementista puhutaan suomalaisissa keskusteluissa, käytetään useimmin ilmauksia tietopääoma, tiedon ja osaamisen johtaminen, tietopalvelu ja tietovarantojen hallinta, tiedonhallinta. Kirjallisuudessa knowledge managementin ominaisuuksiksi mainitaan systemaattisuus, yhdistettävyys, hallinta,

oppiminen ja edistävyys. (Kivinen 2008.) Tässä työssä käytetään termiä ”tiedolla johtaminen”.

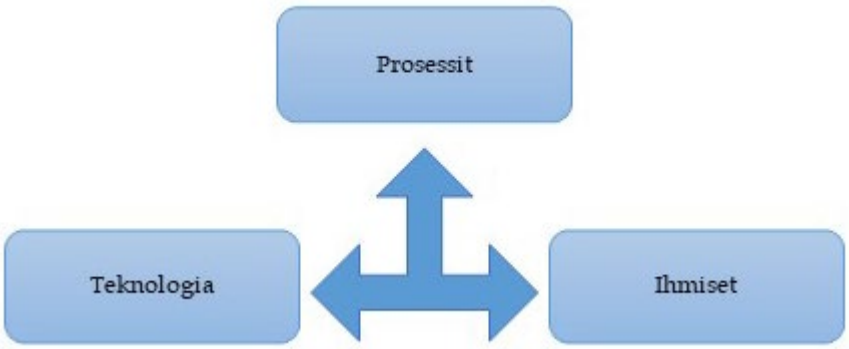
Tiedolla johtamista kuvataan joukoksi menetelmiä, joilla dataa, informaatiota ja tietämystä kerätään, arkistoidaan ja jaetaan. Sitä hyödyntävät eri alojen asiantuntijat järkeistäessään tapahtumia ja ilmiöitä eksplisiittisen ja oman hiljaisen tietonsa pohjalta. Tavoitteena on aiemmin koetun ja tutkitun tiedon hyödyntäminen tulevaisuudessa ymmärryksen kautta. Tiedolla johtamista käytetään useilla toimialoilla tehokkaana tapana kohdata ja suunnitella tulevaisuutta.

Käsitteen pioneereina voidaan pitää Ikujirō Nonakaa ja Hirotaka Takeuchia, jotka kuvasivat käsitettä kirjassaan The Knowledge Creating Company (1995). Käsitettä on hyödynnetty sittemmin niin yksilön, yhteisöjen kuin yhteiskunnan näkökulmista. Nonakan ja Takeuchin (mt.) mukaan uuden tiedon luomisen lähtökohta poikkeaa länsimaisen tietoteorian mukaisesta tiedosta, jota he kuvaavat absoluuttiseksi, staattiseksi ja epäinhimilliseksi tiedon ulottuvuudeksi ja josta heidän mukaansa puuttuu inhimillinen ulottuvuus. He korostavat tiedon sosiaalista vuorovaikutussuhdetta ihmisten ja organisaatioiden välillä.

Ilman tätä vuorovaikutussuhdetta tieto jää informaatiotasolle vaille kontekstin tuomaa inhimillistä ulottuvuutta, jota myös tietämykseksi voidaan kutsua. Ilman inhimillistä tulkintaa, jossa ymmärretään myös toimintaympäristö, on olemassa informaation virheellisen tulkinnan mahdollisuus. Tieto saa inhimillisiä piirteitä, kun siihen liitetään sellaiset yksilön arvokäsitteet kuin sitoutuneisuus ja uskomukset. Ilman tietoa on taas mahdotonta kyetä jäsentämään ympäristöä ja tekemään tavoitteita palvelevia päätöksiä. Englanniksi tätä vaihetta kutsutaan sensemaking-vaiheeksi (Dwivedi 2009) (ks. tarkemmin alaluku 4.2.1.).

Tiedolla johtamisessa ilmiötä ei tarkastella pelkästään teknisestä viitekehyksestä. Prosessilla, toimintaympäristöllä ja toimijoilla on yhtä suuri merkitys. Tiedolla johtaminen on myös tapa tarkastella teknologian vaikutusta toimintaan. Kysymyksenasettelu lähtee enemmän toiminnan tarpeista kuin teknisistä kysymyksistä. Päämääränä on muodostaa dynaaminen vuorovaikutus teknologian ja käyttäjien välille.

Tiedolla johtamisen keskeisin osatekijä ovat toimijat, joilla tässä yhteydessä tarkoitetaan käyttäjiä, sidosryhmiä sekä toiminnallista ympäristöä. Toimintaympäristön kypsyydellä viitataan tässä kontekstissa teknologian käytettävyyteen haasteellisissa ympäristöissä; teknologian tulee täyttää sekä käyttäjien että toimintaympäristön sille asettamat vaatimukset (kuvio 4). Käyttäjien kypsyyteen eli valmiuteen hyödyntää teknologiaa vaikuttavat suuresti esimerkiksi systemaattinen koulutus ja tekninen tuki, jotka varmistavat, että loppukäyttäjät ymmärtävät teknologian mukanaan tuoman lisäarvon. (Bali ym. 2009.)



KUVIO 4. Tiedolla johtaminen (knowledge management) Balin ym. (2009) mallia soveltaen

Modernit informaatio- ja kommunikaatioteknologian innovaatiot tarjoavat tänä päivänä useille eri toimialoille uusia tehokkaita mahdollisuuksia informaation jakamiseen niin sisäisesti omissa organisaatioissa kuin ulkoisillekin sidosryhmille (Wickramasinghe & Bali 2008). Ominaista informaatio- ja kommunikaatioteknologian käyttöönotolle näyttää olevan teknologiakeskeisyys. Teknologinen lähestymistapa tulee yleensä tietojenkäsittelytieteestä, jonka mukaan datasta syntyy erilaisia objekteja käsiteltäväksi eri tietojärjestelmissä. Tietotekniikkaan keskittyvä näkökulma antaa datalle suppeamman merkityksen kuin humanistinen näkökulma, joka keskittyy osaamiseen ja taitoihin sekä näiden hallintaan ihmisten johtamisen ja organisaation näkökulmasta. (Hätilä 2020.)

Klassisesta teknologialähtöisestä orientaatiosta poiketen tiedolla johtamisen lähtökohtana on tarkastella toiminnassa prosessin muutoksia, joita voidaan toteuttaa teknologian avulla. Tietoteknologisen orientaation sijasta tai sen ohella voidaan keskittyä toimijoiden ja toimintaa tukevien sidosryhmien informaationtarpeeseen. Ilmiöitä voidaan tarkastella kokonaisvaltaisemmin, jolloin tarkastelun näkökulma siirtyy teknologiasta prosessin muutokseen sekä toimintaympäristön valmiuteen toteuttaa prosessin muutos teknologian avulla. (Raman ym. 2006.) Teknologialähtöinen ajattelutapa, jossa data palvelee tietojärjestelmiä eikä prosessinmuutosta, ei riitä vastaamaan esimerkiksi kriisinhallinnan monialaisiin ja haastaviin tarpeisiin. Metodina tiedolla johtaminen korostaa ensisijaisesti muutostarpeiden sekä toimijoiden ja toimintaympäristön kypsyyden huomioimista teknologian käyttöönotossa. Teknologia ei ole kehityksen itseisarvo vaan ennemminkin muutoksen mahdollistaja. (Koivula 2008.)

Tiedon käsitteen rakenteellinen jäsennys, jossa tieto on luokiteltu siihen liittyvän inhimillisen, intellektuaalisen prosessoinnin perusteella, on laajasti hyväksytty (Savolainen 1994). Mitä korkeammalle tiedon asteelle edetään, sitä enemmän tieto sisältää inhimillistä ajattelua, työstämistä ja arviointia ja sitä vähemmän sitä voidaan käsitellä ja tuottaa teknisesti irrallisena materiaalina. Tämä on jäsennelty näkemys polusta, joka johtaa viisauteen ja sitä kautta perusteltuun päätöksentekoon. (Raavo 2021.)

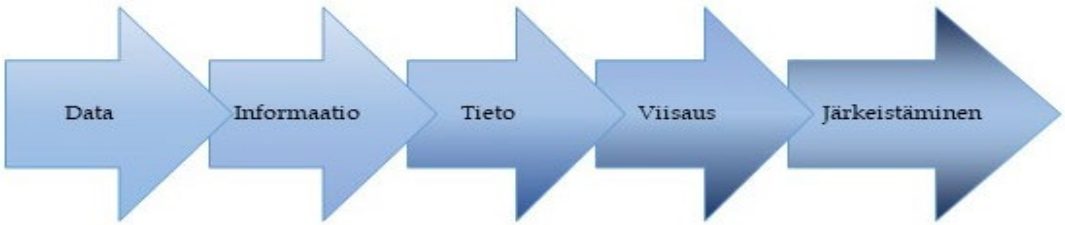
Esimerkiksi Balin ja muiden (2009) mukaan johtamistieteiden määritelmissä tieto voidaan luokitella eri tasoihin, jotka ovat data, informaatio, tieto ja

viisaus. Data on heidän määrityksensä mukaan fyysinen merkki, ”taustakohina”, jolla ei ole merkitystä, koska se jää datan vastaanottajan ymmärryksen ulkopuolelle, ikään kuin kryptiseksi massaksi. Informaatio eli merkitys saadaan asiantuntijan prosessoidessa dataa kognitiivisesti. Tieto taas koostuu uskomuksista, jotka tunnistetaan normatiivisesti ja sosiaalisesti oikeiksi.

Soininen tulkitsee Ackoffin esittämiä määritelmiä (1989, 3–9) seuraavanlaisesti:

> Data määritellään symboleiksi, jotka edustavat objektien ominaisuuksia, tapahtumia ja niiden ympäristöä. Ne syntyvät olemassa olevasta ympäristöstä, mutta ne eivät tuo lisäarvoa ennen kuin ne muodostuvat ymmärrettäväksi. Datan ja informaation ero on siis toiminnallinen, ei rakenteellinen. Informaatio vastaa kysymyksiin, jotka alkavat sellaisilla sanoilla, kuten: kuka, mitä, milloin ja kuinka monta. Tietojärjestelmät tuottavat, tallentavat, hakevat ja käsittelevät tietoja. Informaatio voidaan päätellä datan perusteella. Tieto on tietotaitoa ja se tekee mahdolliseksi informaation muuttamisen ohjeeksi. Viisaus on taasen kykyä lisätä tehokkuutta. Viisaus tuo lisäarvoa, joka vaatii henkistä toimintoa, jota voi kutsua arviointikyvyksi. Eettiset ja esteettiset arvot, joihin nämä viittaavat ovat ainutlaatuisia ja henkilökohtaisia. (Soininen 2021)

Rajeev Bali, Nilmini Wickramasinghe ja Brian Lehaney tuovat teoksessaan Knowledge Management Primer (2009) tiedolla johtamiseen tietojärjestelmänäkökulman. He kuvaavat datan, informaation, tiedon ja viisauden määritelmiä. Heidän näkemyksensä mukaan data ilmenee kryptisenä massana ilman arvoa. Datasta jalostuu kuitenkin informaatiota, ja sen nähdäänkin olevan organisoitua tai strukturoitua dataa. Tämä käsittely muodostaa datasta tietoa, jolla on merkitys, tarkoitus ja yhteyksiä – se siis tekee datasta arvokasta, hyödyllistä ja merkityksellistä (kuvio 5). Tietoa voidaan pitää sekoituksena informaatiota, ymmärrystä, kyvykkyyttä, kokemusta, taitoja ja arvoja, joihin viisaus perustuu.



KUVIO 5. Polku datasta tiedon kautta järkeistämiseen Balin ym. (2009) mallia soveltaen

Datalla tarkoitetaan koodeja, merkkejä ja signaaleja, jotka ilman asiantuntijan tulkintaa jäävät kryptiseksi massaksi vailla merkitystä. Data on siis eräänlaista taustakohinaa, kunnes joku, joka kyseistä dataa ymmärtää, saa sen käsiteltäväkseen. Datasta muodostuu informaatiota, kun sitä kyetään tulkitsemaan. Data voidaan siten nähdä informaation raaka-aineena (Bali ym. 2009). Datan luotettavuudella, oikeellisuudella sekä eheydellä on prosessissa suuri merkitys, sillä informaatio perustuu datan luotettavuuteen.

Informaatio omaksutaan tiedoksi, kun ihminen yhdistää sen osaksi kokemusten kautta syntynyttä hiljaista tietoa tai näyttöön perustuvaa eksplisiittistä tietoa (Nonaka & Takeuchi 1995). Näin tieto on perusteltua ja tätä kautta ymmärrettävissä ja omaksuttavissa. Päämääränä tavoitellaan viisautta (wisdom), jonka

avulla asia tehdään ymmärrettäväksi (sensemaking). Samalla syntyy metaymmärrystä, jonka avulla syntyy uutta tietoa. Viisauteen liitetään myös näkemyksiä hyvästä elämästä ja tiedon käytöstä päämäärien edistämiseen.

Tiedolla johtamisen näkökulmasta tietosuojatyössä datamassaksi voidaan määritellä mm. tietoturvaan liittyvät poikkeamaraportit, jotka asiantuntija voi jalostaa informaatioksi, jota sitten tarjotaan organisaation johdolle. Ennaltaehkäisyn näkökulmasta informaatio on arvokasta silloin, kun siitä jalostetun tiedon perusteella osataan arvioida poikkeamien vaikutukset toimintaan ja estimoida uhan todennäköisyys. Tämän tulisi johtaa ennaltaehkäiseviin toimenpiteisiin poikkeaman varalta.

4.2.1 Tiedon jakaminen ja siiloutuminen

Tiedon jakamiseen liittyy uusien ideoiden keksiminen sekä toimintaperiaatteiden ja -mallien kehittäminen. (Matošková 2016, 9; Wang & Noe 2010.) Tiedon jakaminen on keskeinen tavoite toteutettaessa Nonakan ja Takeuchin (1995) kuvaamaan SECI-mallia.

Soininen (2021) tuo esille, että tiedon jakaminen voi olla haasteellista, koska jos asiantuntijat eivät kykene jalostamaan tietoa informaatioksi, tieto voi olla vain merkityksetöntä datamassaa. Toisaalta tietotaito on jatkuvasti kehittyvää, sillä tiedon siirtyessä henkilöltä toiselle voivat tiedon merkitys ja sen soveltamisen mahdollisuudet kasvaa. Riippuen tarkastelun viitekehyksestä voidaan dataa tulkita useilla eri tavoilla, ja se johtaa parhaimmillaan tietotaidon laajentumiseen. (Lilleoere & Holme Hansen 2011.)

Organisaatiot jakavat tietoa kirjallisesti tai kasvotusten vuorovaikutusverkostoissa muiden asiantuntijoiden kanssa tai dokumentoimalla, järjestelemällä ja tallentamalla tietoa muiden käyttöön (Wang & Noe 2010). Tämä johtaa siihen, että jaettu tieto yhdistyy yksilöiden tiedon kanssa uudeksi tiedoksi ja laajentuneeksi tietämykseksi (Matošková 2016). Ihmisten rooli ja motivaatiot ovat kriittisin osa tiedon jakamisessa (Cummings 2003).

Tiedon jakamisen motivaatiota vahvistavat tai heikentävät esimerkiksi toimijoiden väliset suhteet, vastaanottajan kyky omaksua tai käyttää tietoa sekä vastaanottajan kyky ymmärtää tiedon merkitys kokonaisuuden ja käytännön työn kannalta (Syed-Ikhsan & Rowland 2004, 96). Tiedon jakamisen onnistuminen edellyttää vuorovaikutustaitoja (Paloniemi 2004; Asrar-ul-Haq & Anwar 2016). Tiedon jakamisen esteenä voi olla palkitsemisen puute tai pelko siitä, että tiedon jakamisen yhteydessä menetetään jotain henkisesti, taloudellisesti tai sosiaalisesti (Soininen 2021).

Malkamäen (2017, 135) mukaan uusi teknologia ja fyysinen kohtaaminen luovat tehokkaan johtamiskäytännön ja mahdollistavat tiedon välittymisen eri tasoille. Tiedon saatavuus oikeaan aikaan oikeassa muodossa mahdollistaa yhdenmukaisen näkemyksen käsillä olevasta ilmiöstä (Saumya 2015, 107–108). Tiedon jakaminen riippuu oleellisesti myös siitä, miten kompleksista tieto tai data on (Saumya 2015, 107–108).

Oksmanin (2017) mukaan organisaation prosessien ymmärtämiseen sopii sensemaking-teoria, ”merkityksellistäminen”. Lopputulosten tarkistelun sijaan

fokus on niissä merkityksissä, joita yksilöt ja organisaatiot antavat tapahtumille. Ihmiset yrittävät luoda muutokseen tai kaaostilanteeseen järjestystä ja selittää tapahtumat rationaalisesti. Ennaltaehkäisy on keino päästä tiedon ymmärryksen tasolle mahdollisimman varhaisessa vaiheessa (Aaltonen 2009).

Kaivo-oja (2012) kuvaa sensemakingia ymmärryksen luomiseksi järkeilemisen ja toiminnan kautta. SECI-prosessissa käytettävät taidot, kommunikaatio ja avoin viestintä ovat keskeisiä tekijöitä poikkeamatilanteiden haltuun saamiseksi. Sensemaking-prosessointi on käsillä esimerkiksi silloin, kun eteen tulee jokin yllätyksellinen keskeytys tai muutos. Sensemaking alkaa epävarmuudesta, jota ei ole ennakoitu. Ennen toimintavaihetta ihmiset hahmottavat tilannetta erilaisten vihjeiden, havaintojen, ajatusten ja tietojen perusteella. Hahmottaminen tapahtuu esimerkiksi vertaamalla havaintoja aiempiin kokemuksiin. Näitä kutsutaan myös heikoiksi signaaleiksi (Immonen & Rantanen 2011).

Loisan (2006) mukaan kehitykseen vaikuttavat tekijät voidaan jakaa heikkoihin signaaleihin, trendeihin ja megatrendeihin. Heikot signaalit ovat toimintaympäristöstämme muodostuva epämääräinen datamassa. Mikäli niihin ylipäätään kiinnitetään huomiota, ne havaitaan normaalista poikkeavana ja outona ilmiönä, joka ei ole mallinnettavissa, mikä tekee ilmiöstä vaikeasti ymmärrettävän. Mannermaan (2004) mukaan yleisessä kehityksessä tapahtuu murroksia, joiden havaitsemiseksi tulee kiinnittää huomiota heikkoihin signaaleihin, erityisesti sellaisiin, jotka ovat outoja, epämääräisiä ja kehittymättömiä. Heikkojen signaaleiden tarkkailu ja oikea-aikainen reagointi niihin on haasteellista ja vaatii systemaattista seurantaa.

Ennaltaehkäisyn näkökulmasta heikot signaalit ovat merkityksellisiä. Vaikuttava kriisinhallinta perustuu proaktiivisuuteen ja ennaltaehkäisyyn, ja niitä varten on heikkoja signaaleja kyettävä tunnistamaan ja tulkitsemaan (Immonen ym. 2009; Kreiner ym. 2013). Samaa ajatusta voidaan hyödyntää, kun tehdään sisäänrakennettua ja oletusarvoista tietosuojatyötä. Organisaatiossa tulee olla myös kykyä analysoida objektiivisesti eri tietosuojaskenaarioiden toteutumisen todennäköisyyksiä.

Kun toimitaan ei-toivotun ilmiön, poikkeamien, kanssa tai epävarman tiedon varassa, toiminta on etenemisen ja palaamisen, suunnittelun ja tekemisen vuorottelua (Kaivo-oja 2021). Kuvattu tapahtumaketju voidaan rinnastaa SECI-prosessiin.

Tietosuojatyö on riskilähtöistä (Tietosuoja-asetus 2016/679; Korpisaari ym. 2018; Kaivola 2016); tietosuoja on olemassa siksi, että voidaan ehkäistä ja vähentää tiedon väärin käyttämisen riskejä. Sen vuoksi tässä tutkimuksessa tarkastellaan myös riskienhallintamalleja, joita voidaan käyttää esimerkiksi poikkeamatilanteiden ennakoinnissa.

Vuorela (2013) kuvaa informaatioprosessia tiedon hakemisen ja muistamisen mekanismiksi, jossa tulkinnat määrittelevät tiedon tärkeyden ja merkityksen eri toimijoille. Poliittisella lähestymisellä tunnustetaan eri osapuolien intressit tiedon jakamiselle tai jakamatta jättämiselle. Tehokas tiedon jakaminen on keskeisessä asemassa toiminnan vaikuttavuudessa. (Vuorela 2013.) Oikea-aikainen ja laadukas tieto ja sen jakaminen vähentävät virheitä, nopeuttavat työntekoa ja

tekevät siitä mielekkäämpää ja tehokkaampaa (Stenberg 2012, 140–145). Mikäli toimijat kykenevät tarkastelemaan tilannetta objektiivisesti ja kokonaisvaltaisesti, voidaan myös toimenpiteet optimoida kokonaisuuden kannalta tehokkaasti. (Vuorela 2013.)

Ståhle ja Sotarauta (2002) esittävät, että yksi tietoyhteiskunnan keskeisimmistä ansioista on eittämättä eri organisaatioiden välisen verkostoitumisen myötä syntynyt yhteistyö. Organisatoriset rajat ylittävältä yhteistyöltä odotetaan vaikuttavuutta myös yhteiskunnallisten haasteiden ratkaisemiseksi. Parhaimmillaan tietoyhteiskuntamalli tarjoaa ratkaisuja kollektiiviseen toimintaan. (Ståhle & Sotarauta 2002.) Verkostomaisessa toiminnassa yksiköt kykenevät samalla tekemään laajaa yhteistyötä verkostoissa. Toimijat ovat kuitenkin itsenäisesti vastuussa heille määrätyistä tehtävistä osana kokonaisuutta. Pyrkimyksenä on, että toimijat olisivat itseohjautuvia, mutta prosessit ja hierarkia olisivat tarkasti määriteltyjä kokonaisvaltaisen koordinoinnin näkökulmasta. Tavoitteena on säilyttää toimijoiden väliset vastuualueet sekä johdon aloite- ja ohjauskyky. (Kivekäs 2014.)

Tiedon jakaminen ei välttämättä perustu yleisen hyvän tai kokonaisvaltaisen edun tavoitteluun. Stenbergin (2012) mukaan syyt tiedon jakamiseen voivat vaihdella henkilökohtaisista kollektiivisiin syihin sekä tiedon jakamisen kautta syntyvään lisäarvoon. Tiedon jakamisen motiiveina voivat olla mukavuudenhalu ja pyrkimys päästä helpommalla työtilanteissa sekä tavoite saada enemmän henkilökohtaista etua tilanteesta. Tällaiset motiivit voivat aiheuttaa myös ristiriitoja toimijoiden kesken. Stenberg jatkaa analyysissaan, että tiedon jakamisella on vaikutusta kaikkien osapuolten päivittäiseen toimintaan ja yhteistyöhön. Oikeaaikainen ja laadukas tieto ja sen jakaminen vähentävät virheitä ja nopeuttavat työntekoa tehden siitä mielekkäämpää ja tehokkaampaa. (Stenberg 2012, 140–145.) Tiedon pihtaamisen kulttuuri taas johtaa täysin päinvastaisiin tuloksiin.

Kivekkään (2014) mukaan reaalimaailman verkostoitumisen ja tiedon jakamisen esteenä on siiloutuminen, joka hidastaa toimintaa. Organisaatioissa tapahtuvassa siiloutumisessa on kyse vahvojen ja autonomisuutta tavoittelevien toimijoiden tavoitteenasettelusta. Mikäli organisaation tavoitteet ovat ristiriidassa toimijoiden yhteisten tavoitteiden kanssa, toiminnalla on yleensä yhteistyötä heikentävä vaikutus (Kivekäs 2014).

Tiedostettujen, rakenteellisten siilojen lisäksi on tunnistettavissa tiedostamattomia asenteita, jotka myös aiheuttavat siiloutumista ja vaikeuttavat yhteistyötä eri toimijoiden välillä. Kivekäs tekee omassa tutkimuksessaan osuvan yhteenvedon kuvatessaan, että siiloutuminen on ryhmän, yksikön, systeemin, prosessin tai muun organisaation toimimista eristyksissä muista. Hän myös määrittelee siiloutumisen asenteeksi, ajatusten ja uskomusten luomaksi mielikuvaksi, joka ilmenee ryhmän tai yksikön haluttomuutena jakaa tietoa tai olla vuorovaikutuksessa toisten kanssa. (Kivekäs 2014, 16–17.) Myös toimintaympäristöön syntyvät rajat voivat vaikeuttaa kommunikointia ja yhteisten tavoitteiden saavuttamista. Kyse on nimenomaisesti siitä, kuinka toimintayksiköt älyllisesti ja tunneperäisesti hahmottavat omaa rajallista ja henkilökohtaista suhdettaan asiantuntemukseensa. (Ardichvili ym. 2003.)

4.2.2 Hiljainen tieto ja eksplisiittinen tieto

Nonaka ja Takeuchi (1995) painottavat tietokäsityksessään kognitiivisia prosesseja sekä ihmisen kokemuksen ja luovuuden kautta syntyneen osaamisen, hiljaisen tiedon, merkitystä. Tämä ei poissulje näyttöön perustuvan, eksplisiittisen, tiedon merkitystä. Nämä pikemmin täydentävät toisiaan tiedon ymmärtämisprosessissa. (Nonaka & Takeuchi 1995.)

Nonaka ja Takeuchi kuvaavat hiljaista tietoa kokemuksen kautta syntyneiksi taidoiksi. Hiljainen tieto voidaan jakaa kahteen ulottuvuuteen. Ensimmäinen on ”know how”, johon kuuluvat kokemuksellinen osaaminen (ns. kädentaito) ja taidolliset näkemykset. Toiseen, kognitiiviseen ulottuvuuteen kuuluvat vaikeasti tiedostettavat uskomukset, arvot sekä kaavat, jotka ovat juurtuneet syvälle ihmiseen. Tämä älyllinen ulottuvuus muodostaa tapamme hahmottaa maailmaa. Yksilölliset käsitykset, jotka ovat kulttuurisidonnaisia ja tuntemus- ja kokemuspohjaisia ja joissa intuitio sekä tuntemukset ovat keskeinen osa hiljaista tietoa, muodostavat toimijan arvopohjan ja normit, joilla informaatiota voidaan suodattaa, jäsentää ja tulkita. Tämä tuo väistämättä eri näkökulmia ja ulottuvuuksia saadun informaation perusteella tapahtuvaan päätöksentekoon. (Wickramasinghe ym. 2009, 23–27.)

Parkkilan (2013, 17) mukaan hiljainen tieto on jäänyt vähemmälle huomiolle, koska sen olemassaoloa ei aina tunnisteta eikä sen systemaattinen jakaminen myöskään näin ollen ole suunniteltua. Suomelan (2016; Alasuutari 2011; Pohjalainen 2016) mukaan organisaation kulttuurin tulisi tukea ja edesauttaa hiljaisen tiedon jakamista. Toimiva yhteistyö ja vuorovaikutus ovat keskeisessä roolissa onnistuneessa hiljaisen tiedon jakamisessa. Hiljainen tieto sijaitsee työntekijöiden mielissä ja osaamisessa, ja organisaation tiedonlähteenä sen osuus on merkittävä. Hiljaisen tiedon hyödyntäminen on haasteellista, koska se on sidottu työntekijän kokemukseen, tilanteeseen ja kulttuuriin. Hiljaisen tiedon näkyväksi tekeminen laajentaa siten organisaation tietopääomaa ja parantaa päätöksentekoa. (Iqbal 2021; Stewart & Waddell 2008.) Tiedon merkitys korostuu entisestään, kun toimintaympäristössä tapahtuu muutoksia (Bali ym. 2009).

Soinisen (2021) mukaan työn laadun parantamisessa sekä odottamattomien tilanteiden ratkaisemisessa on olennaista yksilöiden tiedon ja organisaation innovatiivisuuden kehittyminen. Varsinkin suuret organisaatiot hyötyvät tietojohtamisen työkalujen käytöstä toiminnassaan. Mikäli organisaatio haluaa hyödyntää tietoa merkittävänä omaisuuseränä tai taloudellisena resurssina, on sen tiedostettava, miten tietoa luodaan, jaetaan ja käytetään organisaatiossa. Strategiaa laadittaessa ja prosessien kuvauksissa on tunnistettava ja tiedettävä, missä organisaation näkyvä ja hiljainen tieto sijaitsee. Tällä varmistetaan, että tietoa luodaan ja että tieto siirtyy oikeille henkilöille. (Soininen 2021.)

Uuden tiedon luomisessa hiljaisen tiedon rinnalla korostuu täsmällisen tiedon analysoinnin taito. Eksplisiittinen tieto suomennetaan poikkeuksetta käsitteelliseksi tiedoksi. Ominaista eksplisiittiselle tiedolle on, että se saa sääntöihin perustuvan määrämuodon, jota voidaan esittää esimerkiksi matemaattisten tai muiden tieteellisten numeroiden, symbolien ja kaavojen muodossa.

Määrämuotoisuutensa vuoksi sitä voidaan prosessoida ja tallentaa systemaattisesti. Myös fyysiset objektit ovat eksplisiittistä tietoa.

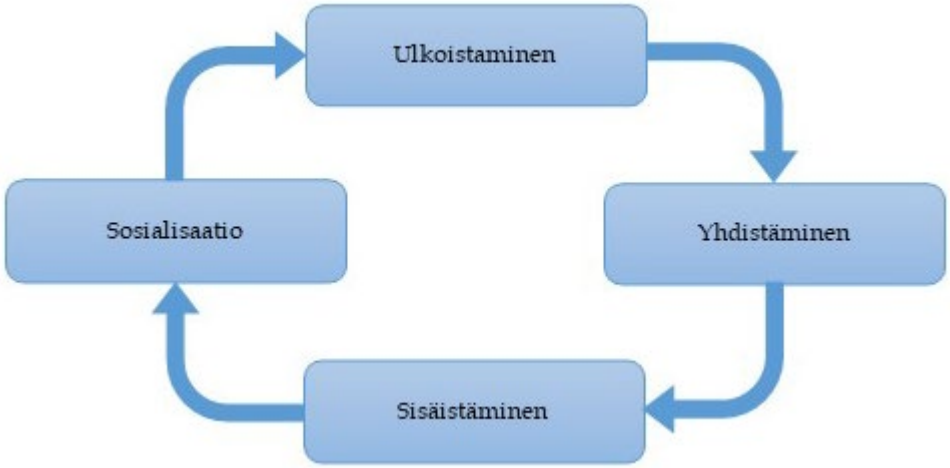
Muodollisen ja järjestelmällisen ominaisuutensa vuoksi eksplisiittinen tieto on operationalisoitavissa, jolloin se toimii luontaisena informaatiojärjestelmien ”raaka-aineena”. Koska eksplisiittistä tietoa on yleensä helppo kerätä, tallentaa, käsitellä ja jakaa erilaisin menetelmin, esimerkiksi ohjelmistojen avulla, on tieto tehokkaasti hankittavissa, hyödynnettävissä ja jaettavissa tietotekniikan avulla. Määrämuotoisuutensa ja helppokäyttöisyytensä vuoksi useimmin käytetyt lähteet ovat eksplisiittisiä, esimerkiksi tietokannoista haetun datan analyysit tai usein toistettujen testien mittausinformaatio. (Dwivedi ym. 2002.)

Tietoon liittyy aina arvonäkökulma. Silloinkin kun puhutaan ns. objektiivisesta informaatiosta, se herättää dataa prosessoivassa toimijassa arvoja, asenteita ja tunteita, jotka perustuvat hänen kokemuksensa kautta syntyneeseen hiljaiseen tietoon. Nämä vaikuttavat merkittävästi siihen, miten informaatiota tulkitaan, miten se ymmärretään ja, ennen kaikkea, miten se vaikuttaa. (Nonaka & Takeuchi 1995.)

4.2.3 Tiedon muunnosprosessi – SECI-malli tiedon jalostamiseen

Ståhle ja Sotarauta (2002), Stenberg (2012) ja Vuorela (2013) kuvaavat hiljaisen ja eksplisiittisen tiedon välisiä muunnoksia, joiden avulla voidaan mallintaa dynaamista prosessia, jossa käsitteellistä ja hiljaista tietoa muunnetaan ja siirretään ihmisten välillä. Prosessi auttaa yksilöitä hyödyntämään omaa sekä ihmisten vuorovaikutuksen tuloksena syntyvää hiljaista tietoa. Mallin avulla voidaan analysoida, millaisia arvoja ja asenteita ihmisen on kehitettävä itsessään, jotta tiedon jakamisprosessi toimisi.

Teoksessaan The Knowledge-Creating Company Nonaka ja Takeuchi (1995) esittelevät SECI-mallin, joka kuvaa hiljaisen tiedon muuntumista näkyvään muotoon ja takaisin hiljaiseksi tiedoksi. Mallin avulla tavoitellaan entistä laadukkaampaa ja systemaattisempaan tiedon jakamisen ja muuntamisen prosessia organisaatiossa. Mallin avulla organisaatio voi paremmin ymmärtää tiedon jakamisen ja muuntamisen eri vaiheet. Malli kuvaa organisaation tiedon muuntumista neljässä eri vaiheessa: tiedon sosialisaatio (socialization), tiedon ulkoistaminen (externalization), tiedon yhdistely (combination) ja tiedon sisäistäminen (internalization). Jokainen vaihe edustaa tietoa siirtävää prosessia, joka muuntaa tietoa yhdestä muodosta toiseen.



KUVIO 6. SECI-malli – tiedon spiraali Nonakan & Takeuchin (1995) mallia soveltaen

SECI-malli (kuvio 6) tarjoaa metodin uuden tiedon oppimiseen ja jakamiseen niin, että parhaimmiksi todetut toimintamallit tulevat samalla tavalla käyttöön läpi organisaation, laajemmin jopa muillakin hallinnonaloilla. Uuden tiedon laaja jakelu edistää organisaatiossa oppimista, ja organisaatiossa syntyvää tietoa voidaan käyttää ongelmanratkaisuun ja päätöksentekoon sekä uuden tiedon luomiseen. Uuden tiedon luonti vaatii organisaation jäsenten vuorovaikutusta ja sosiaalisia suhteita, jotka rikkovat syntyneitä siiloja. SECI-malli tukeutuu vahvasti sekä hiljaisen että eksplisiittisen tiedon jakamiseen uusien asioiden ja ilmiöiden haltuun ottamiseksi organisaatiossa. SECI-malli ei kuitenkaan noussut esille tutkimuksen aikana käydyissä keskusteluissa, mistä voitaneen päätellä, ettei tätä tiedolla johtamisen osa-aluetta käytetä hyväksi tietosuojatyön strategisessa johtamisessa.

Sosialisaatio

Tärkeä osa SECI-prosessia on ainutkertaisen persoonallisen tiedon esittäminen ymmärrettävässä muodossa. Hiljaisen tiedon jakaminen yksilöiden kesken määritellään sosialisaatioksi, jossa kokemuksia vaihdetaan ja niistä opitaan. Toinen hiljaiseen tietoon liitetty tapa siirtää tietämystä on toisten tarkkailu esimerkiksi työssä sekä olemalla ja tekemällä yhdessä. Sosialisaatio edellyttää, että ihminen kiinnostuu toisten osaamisesta ja on motivoitunut kehittämään itseään myös yhdessä toisten kanssa. Hänen täytyy huomata, ettei se, miten hän itse toimii ja työskentelee, ole ehkä ainoa oikea tapa. Tarvitaan nöyryyttä, jotta voidaan oppia toisilta. Hiljaiselle tiedolle on ominaista, että se sisältää erilaisia toimintamalleja, ajattelutottumuksia, toimintakulttuuria, normeja sekä arvoja. (Ståhle & Sotarauta 2002, 5, 40–44; Stenberg 2012, 58–59; Vuorela 2013, 13–14.) Sosialisaatio-vaiheessa luodaan yhteistä hiljaista tietoa jakamalla ajattelumalleja, kokemuksia sekä teknisiä taitoja.

Ulkoistaminen

Jotta hiljainen tieto saadaan laajasti hyödynnettyä, on ilmeistä, että se täytyy ulkoistaa muiden käyttöön. Toisessa vaiheessa hiljainen tieto muutetaan käsitteellisen tiedon muotoon. Ihmisen on motivoiduttava kuvaamaan oma näkemyksensä toisille ja kiinnostuttava siitä, miten toiset asian näkevät. Kun molempien osapuolten motivaatiot kohtaavat, syntyy erinomainen mahdollisuus tuottaa uutta oivallusta. Käytännössä tämä hiljaisen tiedon ulkoistamisprosessi perustuu hiljaisen tiedon artikuloimiseen, jota varten on otettava käyttöön ja kehitettävä ilmaisemisen menetelmiä. (Ståhle & Sotarauta 2002; Stenberg 2012, 58–59; Vuorela 2013, 13–14.)

Ulkoistamisen vaiheessa asiantuntijan oma hiljainen tieto muunnetaan organisaation tai sen sisällä olevan ryhmän yhteiseksi näkyväksi tiedoksi käsitteellistämisen ja artikuloinnin kautta. Käytännössä tietosuojaorganisaation tietosuoja-asiantuntijat jakavat kokemuksen kautta syntynyttä hiljaista tietoa organisaation eri tasojen vaatimusten perusteella. Tieto muutetaan ulkoistamisvaiheessa ymmärrettävään ja tulkittavaan muotoon muiden käyttöön. Tietosuojatyössä organisaation tietosuoja- ja viestintäasiantuntijoilla on tällöin merkittävä rooli. Tietosuojatyön hiljainen tieto näyttää syntyvän ensisijaisesti tietosuoja-asiantuntijoille eikä johdolle, vaikka tietosuojatyön kokonaisvastuu onkin tietosuoja-asetuksen mukaan juuri organisaation johdolla (Korpisaari ym. 2018).

Yhdistäminen

Kolmannessa vaiheessa on yksilötasolla nähtävä, miten uusi käsitteellinen tieto, joka on yhteistyöllä saatu esiin, hyödyttää sekä omaa että laajimmillaan koko organisaation innovatiivisuutta, tietopääoman kasvua ja uusien tuotteiden kehittämistä. Yhdistäminen tarkoittaa käsitteellisen tiedon muuntumista uudenlaiseksi käsitteelliseksi tiedoksi. Esimerkiksi käsitteellisen tiedon aikaisemmasta poikkeava tapa yhdistää, ryhmittää ja järjestää tietoa voi johtaa uuteen käsitteelliseen tietoon. Avainasia on kommunikaatio ja tiedon systematisointi. (Stenberg 2012, 58–59; Vuorela 2013, 13–14.)

Olennaista on uuden käsitteellisen tiedon yhdistäminen vanhaan. Tätä varten kerätään käsitteellistä tietoa organisaation sisältä tai ulkoa ja yhdistellään, muokataan tai prosessoidaan siitä uutta tietoa. Toiseksi näin saatua uutta käsitteellistä tietoa levitetään organisaatioon tiedottamisen eri keinoin esimerkiksi esitysten ja kokousten yhteydessä. Tietoa tulee arvioida ja käsitellä suunnitelmien ja raportoinnin avulla niin, että organisaatio voi konkreettisesti hyödyntää tietoa tästä eteenpäin.

Sisäistäminen

Uusi tieto sisäistetään SECI-prosessin neljännessä vaiheessa organisaation hiljaiseksi tiedoksi. Uuden tiedon sisäistämisprosessi tapahtuu, kun käsitteellinen (eksplisiittinen) tieto muuntuu organisaation hiljaiseksi tiedoksi. Tässä vaiheessa sekä uuden tiedon hyödyntäminen että sen levittäminen ja mieltäminen organisaatiolle tärkeäksi resurssiksi laajenevat entisestään.

Yhdistämisvaiheessa ulkoistettu eksplisiittinen tieto kootaan esimerkiksi käsitejärjestelmiksi. Kun tieto on saatu eksplisiittiseen muotoon, voidaan sillä rikastaa aiemmin kerättyä tietoa. Tässä vaiheessa muodostunutta informaatiota analysoidaan ja jäsennetään tiedoksi.

Tietosuojatyössä yhdistämisvaihe on merkityksellinen, sillä päätöksentekohetkellä asiantuntijalla tulee olla käytössään juuri se relevantti tieto, joka tukee päätöksentekoa parhaiten. Sisäistämisvaiheessa tietosuojatyössä sisäistetään tietoa ja uudelleen muotoillaan toimintaa tukeutuen uuteen, näyttöön perustuvaan tietoon, jolloin tämä uusi tieto integroituu organisaation toimintaan ja rutiineihin ja nostaa tietosuojan valmiutta ja kypsyystasoa. Sisäistämisellä tavoitellaan sitä, että tietosuojapolitiikka sekä tilannekuva ymmärretään organisaation johdon eri tasoilla samalla tavalla. Sisäistämisvaiheessa tulee myös huomioida se tosiasia, että eri toimijat tarvitsevat usein eri informaatiota. Tämä väistämättä tarkoittaa sitä, että informaatio voi olla yhdelle toimijalle mitäänsanomatonta kryptologiaa ja toiselle toimijalle mitä merkityksellisintä tietoa. Yksilön sisäistäessä tietoa edellä kuvatusti prosessi jatkuu spiraalina takaisin sosialisaatioon. Näin tiedon määrä kasvaa ja yksilöiden aiemmat käsitykset pääsevät tarpeen tullen muuttumaan.

Yhdistämisvaiheessa yhdistellään prosessissa syntyneen tiedon osia uusiksi kokonaisuuksiksi. Tällöin käytännössä organisaation eri tasoilla toimivat resurssit hyödyntävät merkityksellistä tietosuojainformaatiota omista näkökulmistaan. Kun varmistetaan, että eri tasojen toimijat hyödyntävät heille merkityksellistä tietosuojatietoa, päästään tilanteeseen, jossa tarvittava tieto kohtaa kulloisessakin tilanteessa oikean resurssin. SECI-malli siis omalta osaltaan auttaa purkamaan sitä informaatiotulvaa, joka myös koetaan oman toiminnan kannalta epärelevantiksi tiedoksi.

4.2.4 Tiedolla johtaminen tutkimuksen kehikkona

Marr (2010) on esittänyt tiedolla johtamisen mallin (kuvio 7). Sen kussakin vaiheessa esitetään joukko ohjeita ja kysymyksiä, jotka auttavat tiedolla johtamisen onnistumista organisaatioissa.

KUVIO 7. Tiedolla johtamisen malli Marrin (2010, 30) mallia soveltaen

Marrin (2010) mukaan tiedolla johtaminen voidaan jakaa seuraavaan viiteen vaiheeseen:

1. Määrittele tavoitteet ja niille tietotarpeet. – Tietosuojatyössä on tässä vaiheessa tärkeää ymmärtää organisaation tietosuojapolitiikkaan kirjatut tavoitteet sekä niiden hallintakeinot, sillä ne ohjaavat tiedolla johtamisen prosessia. Lisäksi on varhaisessa vaiheessa tunnistettava eri toimijoiden vastuut ja velvoitteet henkilötietojen käsittelyssä. Näin varmistetaan, että analysoitavat tiedot ovat relevanttia tietoa eri päätöksentekijöille. Samalla varmistetaan, että organisaatiossa johdetaan toimintaa relevantilla tiedolla.
2. Kerää määritelty tieto. – Tässä vaiheessa varmistetaan, että kerätty ja jäsennelty tieto on oikeaa; sen pitää palvella kohdassa 1 esitettyä vaatimusta. Organisaatiossa arvioidaan, onko data oikeassa muodossa ja mikä on paras käsittelytapa. Tässä vaiheessa asiantuntija analysoi dataa ja se alkaa saada ymmärrettävän muodon. Data voi olla myös laadullista (kuvia, ei-strukturoitua dataa, kuten suunnitelmia jne.).
3. Analysoi aineisto ja tee siitä oivalluksia. – Tässä vaiheessa informaatiosta tehdään relevantteja oivalluksia, havaintoja. Analysoidusta datasta poimitaan merkitykselliset asiat informaatioksi. Analyysin täytyy tuottaa informaatiota, joka tukee organisaation strategisia tavoitteita (vaihe 1).
4. Esitä ja siirrä tietoa. – Tämä vaihe on yhteydessä vaiheen 3 tuottamaan relevanttiin tietoon. Relevantti tieto esitetään ja jaetaan tarkoituksenmukaisella tavalla päätöksentekijöille.
5. Tee tietoon perustuvia päätöksiä. – Tässä vaiheessa varmistetaan, että päätöksenteko tapahtuu oikean tiedon perusteella. Usein käy niin, että organisaatiossa joudutaan kysymään, miten luodaan tietämyksestä tekoihin -kulttuuri.

Tiedolla johtamisen onnistumisen yksi edellytys on, että kaikilla toimijoilla on yhteneväinen käsitys tiedon kontekstista sekä yhteiset arvot, kulttuuri ja uskomukset. Tietosuojatyössä nämä reunaehdot toteutuvat silloin, kun eri toimijoilla, rekisteröidyillä, rekisterinpitäjillä sekä tietojenkäsittelijöillä on yhteiset näkemykset henkilötietojen käsittelyyn liittyvistä rooleista, vastuista ja velvoitteista. Stenbergin (2012, 21, 23, 238–239) mukaan tiedolla johtamisen kompastuskivenä on usein organisaation tietotarpeiden määrittely. Tietosuojatyössä yhteinen näkemys muodostuu, kun eri toimijat ovat yhtä mieltä käytettävistä standardeista, kriteereistä sekä ohjeista.

Tiedolla johtamisen onnistumisen lähtökohtana on organisaation johdon syvällinen ymmärrys toimintaympäristöstä ja sen muutoksista, tässä tapauksessa EU:n tietosuoja-asetuksen mukanaan tuomista velvoitteista julkishallinnossa.

Ahosen (2020) mukaan virastojen valmius ja maturiteetti tiedolla johtamiseen vaihtelevat merkittävästi ja myös tiedolla johtamisen käsite ymmärretään hyvinkin eri tavoin. Samaan tulokseen tullaan, kun tiedolla johtamista tarkastellaan Valtorin tietosuojatyössä sekä myös laajemmin valtionhallinnossa.

Edelleen Ahosen mukaan valtionhallinnon tulisi kohdistaa omaan toimintaansa toimenpiteitä, jotta analyyttisten sekä johtavien analyyttisten organisaatioiden osuus saataisiin kasvamaan nykyistä suuremmaksi. Tiedolla johtamisen valmiuksia parantavia toimenpiteitä on suositeltavaa kohdistaa koko organisaatioon. Käytännössä olisi integroitava analytiikkatoimintaa, kuitenkin niin, ettei organisaatiorakenteeseen synny siiloja siten, että johto toimisi esimerkkinä tiedolla johtamisen hyödyntämisessä johtamisprosesseissa sekä ilmiöiden ja tilannekuvien analysoinnissa. (Ahonen 2020.)

4.3 Kriisinhallinnan menetelmät tietosuojan tukena

Haikan (2017) mukaan globaalissa liiketoiminnassa, osana organisaatioiden strategista johtamista sekä operatiivista toimintaa, on syytä huomioida kriisinhallinnan teoriat. Viimeaikaisen globaalin kehityksen vuoksi kriisinhallinnan oppeja on jouduttu ottamaan käyttöön ja niiden tarpeellisuus tiedostetaan yhä vakavammin.

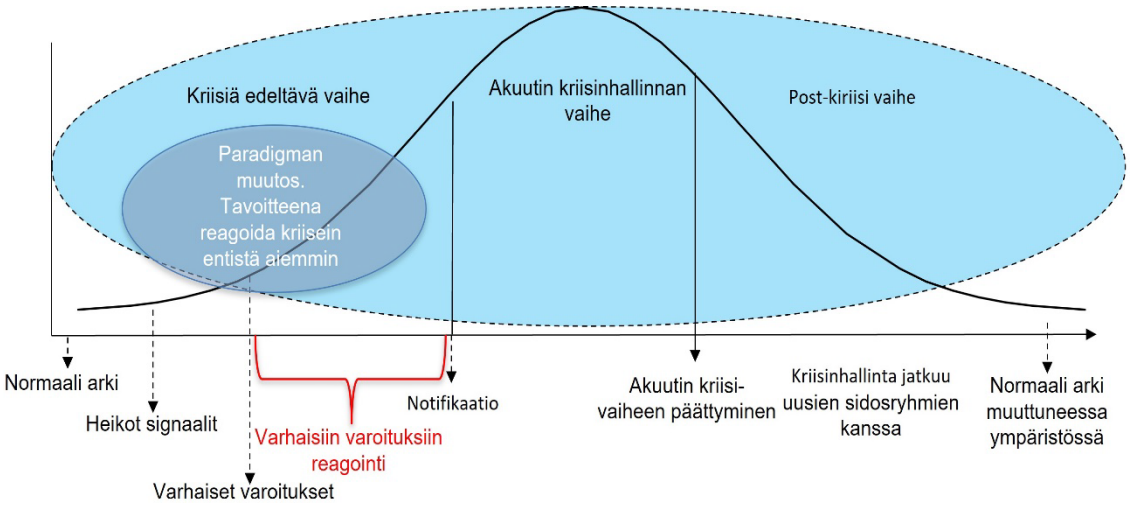
Vakavien tietosuojaongelmien välttämiseksi on syytä perehtyä kriisinhallintatyöhön ja hakea siitä jopa ratkaisumalleja, sillä kriisinhallintatyössä puhutaan ennakoinnin, heikkojen signaalien ja varhaisten varoitusten merkityksestä potentiaalisten kriisien ennaltaehkäisyssä ja haltuunotossa (Immonen ym. 2009).

Riskiperusteisella lähestymistavalla suhteutetaan tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet siihen riskiin, joka henkilötietojen käsittelystä aiheutuu rekisteröidyn oikeuksille ja vapauksille. Tällä pyritään mitoittamaan toimenpiteet kulloinkin henkilötietojen käsittelyyn liittyvän riskin mukaisesti. Jotta rekisterinpitäjä voi toteuttaa asetuksen sisäänrakennettua ja oletusarvoista tietosuojaa, on rekisterinpitäjän arvioitava henkilötietojen käsittelyyn liittyvät riskit. Työ on rekisterinpitäjän vastuulla, ja se kattaa henkilötietojen koko

käsittelyketjun tietojenkäsittelijöihin ja tietojen alikäsittelijöihin asti. (Talus ym. 2017, 16.)

Tietosuojatyössä kriisinhallinta tarkoittaa entistä systemaattisempaa poikkeamien ennakointia, niihin varautumista sekä niitä koskevan tiedon jakamista. Tavoitteena on estää tietoturvan häiriöiden eskaloituminen kriiseiksi. (Gürsoy ym. 2022.)

Tässä tutkimuksessa hyödynnetään Immosen ja muiden (2009) kuvaamaa inhimillisen turvallisuuden kriisikäyrää (kuvio 8), johon on myös kuvattu kriisin kulku eri vaiheineen. Sen avulla tietosuojatyössä päästään prosessoimaan tietosuojapoikkeamia preventiivisesti.



KUVIO 8. Kriisin eri vaiheet Immosen ym. (2009) mallia soveltaen

Makrotasolla kriisit voidaan kuvata normaalijakaumalla, johon sijoitetaan kriisin eri vaiheet. Yhteiskuntien normaaliin arkeen kuuluu luontaisesti pieniä häiriötiloja ja poikkeamia. Tilanteen muuttuessa poikkeukselliseksi ja ei-toivotuksi voidaan tunnistaa vaiheet ennen kriisiä (prior crisis), kriisin aikana (during crisis) sekä kriisin jälkeen (post crisis). Kriisikäyrän alkupäässä ihmiset elävät normaalia arkeaan, kuitenkin jo kriisistä kertovien heikkojen signaalien ympäröiminä. Tilanteen eskaloituessa alkaa eri alojen asiantuntijoille tihkua heikkojen signaalien synnyttämää dataa.

Jossakin vaiheessa kriisiä saavat viranomaiset ilmoituksen ei-toivotusta tilanteesta (Immonen & Rantanen, 2011, kuvio 8), joka käynnistää asianmukaiset toimenpiteet ei-toivotun tilanteen haltuun saamiseksi (Immonen & Rantanen, 2011). Kriisin saavutettua lakipisteensä se alkaa laantua joko luontaisesti tai ihmisten tekemän intervention ansiosta. Lopulta yhteiskunnat pyrkivät jatkamaan toimintaansa syntyneessä uudessa tilanteessa. Huomionarvoista on, etteivät kriisit ole yksittäisiä tapahtumia. Kriisikäyriä syntyy useita sekä yhtä aikaa että sykleissä kriisien eri osa-alueille.

Tietosuoja- ja tietoturvatyössä kriisi-sanan sijaan käytetään yleensä sanaa poikkeama. Tarkasteltaessa laajoja, vakavaksi luokiteltuja poikkeamia voidaan huomata, että ne täyttävät kriisin kriteerit. Tämä vuoksi tässä työssä

tarkastellaan, miten kriisinhallinnassa sovellettavia metodeja voisi hyödyntää osana oletusarvoista ja sisäänrakennettua tietosuojatyötä.

Kriisit saattavat laannuttuaankin jäädä kytemään. Tietoturvatyössä tämä ilmiö korostuu. Lähihistoriassa on useita esimerkkejä siitä, että ulkopuolinen osapuoli on tunkeutunut jopa valtiollisiin tietojärjestelmiin ja kaapannut pitkiksikin ajanjaksoiksi luottamuksellisia tietoja sen omistajan huomaamatta.

Yksi esimerkki tästä on ulkoministeriön tietoverkkoon vuonna 2013 tehty kyberhyökkäys, josta Helsingin Sanomat uutisoi seuraavasti:

> Ulkomaisten tiedusteluelinten epäillään vakoilleen ulkoministeriön tietoliikennettä. Supo tutkii tietomurtoa törkeänä vakoiluna. HS:n tietojen mukaan ulkoministeriön tietoverkkoihin iski useita ulkopuolisia tunkeutujia. Käytännössä tunkeutujat ottivat ministeriön verkon täysin haltuunsa. Osa heistä toimi verkossa vuosia. (Helsingin Sanomat 2013)

Kriisinhallinnan strategioissa ennaltaehkäisyllä on keskeinen rooli. Ennaltaehkäisy perustuu sekä eksplisiittiseen tietoon että kokemuksen, uskomusten ja kulttuurien kautta syntyneeseen hiljaiseen tietoon (Nonaka & Takeuchi 1995). Ennaltaehkäisyllä pyritään estämään tilanteen pahenemista poistamalla riskitekijät tai vähentämällä riskejä eli mitigoimalla vaikutuksia hallittavalle tasolle. Tietosuojatyössä päämääränä on, että tiedon omistaja, rekisterinpitäjä, hyväksyy vielä jäljelle jäävien riskien eli jäännösriskien hallintakeinot. Ennaltaehkäisevän toiminnan tulee perustua validiin informaatioon. Toiminnan keskeisin instrumentti on näyttöön perustuva eksplisiittinen tieto, jota tarvitaan syy-yhteyden varmistamiseen.

Potentiaalisesta uhasta kertovaa dataa skannataan useasta eri lähteestä. Koska tietosuojatyön vaatimuksia toteutetaan hallinnollisin, fyysisin sekä teknisin tietoturvaratkaisuin, voidaan pragmaattisena välineenä eksplisiittisen raakadatan keräämisessä pitää tietoturvallisuuden todentamisprosesseista syntyviä tietoturva-arviointiraportteja. Raaka-datan keruulle on olemassa kansainvälisiä standardeja (ISO 27000 -sarja). Suomessa Puolustusvoimat sekä Traficomin Kyberturvallisuuskeskus ovat myös julkaisseet kriteeristöjä (KATAKRI 2015, PiTuKri) tukemaan valtion toimijoita ICT-palvelujen käyttöönotossa, vaatimusmäärittelyiden arvioinnissa sekä systemaattisen tietoturvan suunnittelussa ja todentamisessa (Stenbäck 2020; Sillanpää 2021).

Syy-yhteyden varmentamisen jälkeenkin poikkeamiin kohdistuvien ennaltaehkäisevien toimenpiteiden toteuttaminen käytännössä voi olla haasteellista, koska kriiseihin liittyy usein erilaisia intressejä. Eri intressipiireillä on oma näkemyksensä kontrollin tarpeesta, toteuttamisesta sekä keinoista. Ennaltaehkäisyn tavoitteiden ja toimenpiteiden tuleekin olla rekisterinpitäjän hyväksymiä. Eettiset, juridiset sekä kulttuuriset tekijät ratkaisevat globaalissa liiketoiminnassa, miten toimintaan ja toimijoihin suhtaudutaan.

Jossakin vaiheessa prosessin aikana, joko luontaisesti tai ihmisen tekemän intervention ansiosta, alkaa kriisin eskaloituminen kääntyä laskuun. Tämän jälkeen kriisistä kärsineet osapuolet pyrkivät jatkamaan elämäänsä uudessa tilanteessa. Kriiseille on myös tyypillistä, että ne muuttavat muotoaan ja seuraavat toisiaan. Jotta nämä ei-toivotut tilanteet olisivat saatavissa haltuun, on

tähdellistä, että eri asiantuntijat tekevät yhteistyötä ja jakavat datasta jalostettua informaatiota mahdollisimman varhaisessa vaiheessa.

Kriisin kehityskaaren alkuvaiheessa alkaa ympäristöstä nousta erilaisia heikkoja signaaleja (weak signals) ei-toivotun tilanteen piirteistä (Kaivo-oja 2012, 206–217). Nämä heikot signaalit syntyvät useista eri lähteistä. Haasteena onkin koota, tulkita, jakaa ja ymmärtää kertynyt data niin, että siitä on tulkittavissa, mikä data jää taustakohinaksi ja mistä on potentiaalia syntyä varhaisia varoituksia. On myös kriittisesti varmistauduttava datan alkuperästä ja sen oikeellisuudesta ja eheydestä (Immonen ym. 2008; Koraeus 2008).

Kriisinhallinta voidaan kuvata kriittisessä tilanteessa sarjaksi toimintoja, jotka on toteutettava hallitsemattoman eskaloitumisen välttämiseksi. Kirjallisuudessa näitä toimintoja kuvataan ymmärryksen (sense making), päätöksenteon (decision making) sekä selvityksen (meaning making) tasoiksi (Koraeus 2008).

Heikot signaalit ja varhaiset varoitukset ilmaantuvat ennen kuin virallinen ilmoitus tilanteesta kohtaa viranomaiset. Päätöksenteko alkaa yleensä vasta silloin, kun ilmoitus saavuttaa viranomaiset. Kriittinen vaihe on siis ajanjakso, joka alkaa heikkojen signaalien ilmaantumisesta ja päättyy silloin, kun asiantuntija kykenee tekemään niiden perusteella johtopäätöksiä. Mitä pidempi tämä ajanjakso on, sitä enemmän jää kriisin eskaloitumiselle tilaa. On selvää, että mitä kauemmin kriisi kehittyy, sitä enemmän resursseja ja aikaa vaaditaan tilanteen haltuun saamiseksi. Kriisi voi myös ehtiä muuttaa muotoaan. (Muhren ym. 2008; Immonen & Rantanen 2011.)

Heikkojen signaalien vaihe

Jokapäiväinen toimintaympäristömme on tulvillaan erilaista dataa, joka kuitenkin suurimmaksi osaksi koetaan taustakohinana. Siihen ei juurikaan tunneta tarvetta reagoida (Ansoff 1975). Heikkojen signaalien analyysin kehittäjänä pidetään Igor Ansoffia (1975), joka määritteli heikot signaalit varoituksiksi, jotka eivät ole kyllin täsmällisiä vaikutusten arviointiin ja päätöksentekoon. Jos joku jostain syystä kiinnostuu datasta, sitä aletaan tulkita informaationa.

Samalla logiikalla voidaan tarkastella heikkoja signaaleja, joita ”leijuu” jatkuvasti ympäristössä yhteiskunnan eläessä normaalia elämäänsä. Tietoyhteiskunnan aikakautena heikoiksi signaaleiksi tunnistettavaa dataa on alkanut muodostua useista eri lähteistä, kuten mittaussensoreista, monitoreista, uutisista, internetistä sekä sosiaalisesta mediasta. Reunaehtojen täytyttyä data alkaa herättää asiantuntijoiden mielenkiinnon, mikä johtaa datan tulkintaan. Tällöin data alkaa saada merkitystä ja siitä syntyy informaatiota. (Jalonen 2015.)

Mikäli asiantuntija havaitsee datassa jotakin poikkeavaa, hän reagoi siihen ilmoittamalla siitä asianmukaisesti ympäristölleen. Samoin toimitaan heikkojen signaalien kanssa ei-toivotuissa tilanteissa. On ilmeistä, että yhteiskunnan tuottamaa dataa voidaan tulkita ja usein tulkitaankin väärin tai jätetään kokonaan huomioimatta. Tähän haasteelliseen tilanteeseen tulisi kriisinhallinnan protokollan kyetä vastaamaan niin, että varmistetaan yhteiskunnasta nousevien ei-toivottujen heikkojen signaalien päätyminen asiantuntijoiden arvioitaviksi.

Varhaiset varoitukset -vaihe

Kirjallisuus näyttää käyttävän varhaiset varoitukset -käsitettä varsin laajasti, mutta sen tarkkaa määritelmää on vaikea löytää. Heikot signaalit nähdään yleisesti merkkinä muutoksesta kohti tuntematonta (Kaivo-oja 2012), ja varhaiset varoitukset nähdään päätöksentekoprosessin ensimmäisenä vaiheena, jolloin tilanteeseen reagoidaan. Heikkojen signaalien vahvistuttua varhaisiksi varoituksiksi alkaa organisaatioissa mitä todennäköisimmin kehittyä strategia tilanteen haltuun saamiseksi. Kun varhainen varoitus on tunnistettu, tulisi olla olemassa suunnitelmat tilanteen laimentamiseksi, jotta ei-toivotun tilanteen eskaloitumiselta erityyppisiksi kriiseiksi vältytään. Kirjallisuus myös osoittaa, että mitä kauemmin tilanne eskaloituu ilman interventiota, sitä enemmän tuhoa ja epävarmuutta on odotettavissa (esim. Mustonen 2015, 5–7).

Heikot signaalit ja varhaiset varoitukset on kriisinhallinnassa erotettu toisistaan. Tilanteissa, joissa epävarmuus on päätöksenteolle tunnusomaista, heikkojen signaalien modifioituminen varhaisiksi varoituksiksi on päätöksentekijöille tärkeää (Immonen & Rantanen 2011). Tiedolla johtamisen käsitteissä määritellään datan ja informaation väliseksi eroksi se, että ympäristöstämme muodostuva data näyttää kryptiseltä massalta, kunnes asiantuntija tulkitsee sen informaatioksi ja tiedon perustaksi. Ei-toivotuissa tilanteissa syntynyt informaatio saa negatiivisen arvolatauksen, jolloin sen pohjalta tehdään ensimmäiset varhaiset varoitukset.

Tässä tutkimuksessa heikkojen signaalien ja varhaisten varoitusten erona pidetään niiden informaatioarvoa: heikot signaalit muuttuvat varhaisiksi varoituksiksi siinä vaiheessa, kun pohjana oleva data pystytään muuntamaan informaatioksi ja sen pohjalta osoitetaan poikkeamia raja-arvoista. Haasteellista oletusarvoisen ja sisäänrakennetun tietosuojan periaatteiden juurruttamisessa on heikkojen signaalien ja varhaisten varoitusten tunnistaminen sekä taito tulkita ja arvioida niiden perusteella poikkeamien aiheuttamien uhkien todennäköisyyksiä.

Haasteeksi myös näyttää muodostuvan tietämyksen jakaminen (knowledge sharing). Siinä tiedon siiloutuminen sekä esteet datan päätymisessä asiantuntijoiden arvioitaviksi vaikuttavat olevan keskeisiä pullonkauloja (Stenberg 2012). Tutkijalle syntyneen ymmärryksen perusteella looginen yhteenveto on, että varhaisten varoitusten vaihe on oikea hetki päättää, onko interventiolle tarvetta.

5 TUTKIMUSOTE JA -MALLI

Tapaustutkimuksen kohteen ollessa Valtion Tieto- ja viestintäkeskus Valtorissa toteutettava tietosuojatyö ja European Data Protection Boardin (EDPB) tunnistaessa tietosuojaan liittyvän kompleksisuuden yhdeksi pilvipalveluiden käyttöönoton haasteeksi valtionhallinnossa on perusteltua todeta, että tämä työ on tiukasti kiinni merkittävässä kansainvälisessä ilmiössä (Närhinen 2022). Nämä lähtökohdat ovat luoneet perusteen väitöstyössä käytetylle tutkimusmetodille.

Tieteellisen tiedon päämääriin kuuluvat teoreettinen pyrkimys totuuteen (pl. tarkoituksella yksinkertaistetut mallit), soveltamiskelpoisen tiedon etsintä sekä uuden tiedon tuottaminen. Laudanin (1978) mukaan tieteen teorialle totuus ei ole itsetarkoitus, vaan se, että uusi tutkimustieto lisää ongelmanratkaisukykyä. Niiniluodon (1984) esittämän tieteellisen tiedon määritelmän mukaan aina ei päästä eksaktiin totuuteen, ja malleja usein yksinkertaistetaan tarkoituksella poikkeamaan totuudesta (Iivari 2023; Siponen & Klaavuniemi 2021), mutta tieteellinen tutkimus tuo pääsääntöisesti uutta tietoa. Tämän pohjalta voidaan todeta, että myös tiedolla johtamisen kehitys vaatii sekä eksplisiittisen eli käsitteellisen tiedon että kokemuksen kautta syntyneen hiljaisen tiedon yhdistämistä ja analyysia sekä näiden tulkintaa uuden tiedon tuottamiseksi.

Neilimon ja Näsin (1980) mukaan konstruktiivinen tutkimusote on hyvin lähellä päätöksentekometodologista tutkimusotetta. Konstruktiivinen tutkimus kuuluu soveltavan tutkimuksen piiriin, jolle on ominaista uuden tiedon tuottaminen. Ensisijaisesti soveltavan tiedon tuloksia arvioidaan niiden pragmaattisen relevanssin näkökulmasta. (Niiniluoto 1989.) Halosen (2019) tulkinnan mukaan konstruktiolla haetaan ratkaisua tiettyyn eksplisiittiseen ongelmaan.

Konstruktiivinen tutkimus tarkoittaa ongelmanratkaisua mallin, kuvion, suunnitelman, organisaation, koneen tai muun vastaavan rakentamisen avulla. Tieteellisessä tutkimuksessa konstruktion menetelmä on eniten käytössä matematiikassa, kielitieteessä, lääketieteessä sekä insinööritieteissä (Kasanen ym. 1991). Konstruktiivisessa tutkimuksessa korostuvat luovuus ja innovatiivisuus sekä heuristisuus, ja siinä edellytetään aina tutkimuksen tuloksen toimivuuden nimenomaista testaamista käytännössä (Halonen 2019).

Konstruktiivisen tutkimusotteen soveltaja hyötyy organisatoristen prosessien syvällistä ymmärtämistä. Kyseinen näkökulma korostuu nimenomaan tässä tutkimuksessa, jossa tavoitellaan mahdollisimman pragmaattista tulosta toteuttamalla esiin nousevat muutostarpeet käytännön tasolla. (Halonen 2019, 67.) (Taulukko 1.)

TAULUKKO 1. Joitakin yleisimpiä tutkijoiden esittämiä tutkimusotteita (Halonen 2019, alkuperäinen jaottelu Neilimo & Näsi 1980).

Tutkimusote	**Kuvaus**
Käsiteanalyyttinen	Analyysin ja synteesin avulla tuotetaan uusia käsitteitä ja malleja. Tutkimuskohteina voivat olla normit ja arvot, ja tutkimustulokset saattavat olla toteavia tai suosittelevia.
Nomoteettinen	Tavoitteena on löytää lainalaisuuksia. Kiinnittynyt voimakkaasti positivistiseen traditioon.
Päätöksentekometodologinen	Tavoitteena on osoittaa tietty metodi, joka ratkaisee määritellyn ongelman.
Toiminta-analyyttinen	Tavoitteena on ymmärrys. Lähellä hermeneutiikkaa.

Kasanen, Lukka ja Siitonen (1991) ovat esittäneet konstruktiivisen tutkimuksen jakautuvan kuuteen vaiheeseen. Tämän tutkimuksen konstruktio soveltaa kyseiset vaiheet:

1. **Relevantin ja tutkimuksellisesti mielenkiintoisen ongelman etsiminen** liittyy tässä tutkimuksessa EU:n yleisen tietosuoja-asetuksen vaatimusten toteuttamiseen valtionhallinnossa. Tietosuoja-asetuksen voimaantulon myötä virastojen tulee huomioida rekisteröityjen oikeuksien ja vapauksien toteutuminen kokonaan uudella tavalla.
2. **Esiymmärryksen hankkiminen kohteesta** tapahtuu tutustumalla aiheesta aiemmin tehtyyn tutkimukseen.
3. **Innovaatiovaiheen ja ratkaisumallin konstruoiminen** tarkoittaa tässä tutkimuksessa esiymmärryksen kautta tehtyjä teoreettisia ja käytännöllisiä huomioita oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamisesta.
4. **Havaintojen varmistaminen** tapahtuu vertaamalla kohdeorganisaatiossa tehdyn määrällisen tutkimuksen tuloksia haastattelun tuloksiin.
5. **Ratkaisun tieteellinen uutuusarvo** osoitetaan esittelemällä kriisinhallinnassa ja tiedolla johtamisessa käytössä olevien metodien potentiaali havaittujen haasteiden ratkaisemisessa. Konstruktion uutuusarvo on siinä, ettei tiedolla johtamisen yhteyttä oletusarvoisen ja sisäänrakennetun tietosuojan vaatimuksiin ole esitetty aikaisemmin.
6. **Ratkaisun soveltamisalueen laajuutta** tarkastellaan alistamalla esille nousseet uudet innovaatiot eri virastojen tietosuoja-asiantuntijoiden kommentoitavaksi.

Lukka (2006) toteaa, että ajan saatossa alkuperäisestä konstruktiivisesta tutkimusmenetelmästä on muodostunut erityyppisiä metodisia käytäntöjä ja konstruktiivinen tutkimusotteen potentiaalinen soveltamisalue on laaja. Samalla hän tuo esille, että konstruktiivinen tutkimusote on laajasti sovellettu eri aloilla,

kuten esimerkiksi tietojenkäsittelytieteessä ja lääketieteessä, joissa on käynnissä useita tutkimuksia, joissa hyödynnetään konstruktiivista tutkimusotetta (Kasanen ym. 1991; vrt. Mattessich 1995).

Lukka (2000) on myös esittänyt konstruktiivisen tutkimuksen viisi vaiheisena, jossa tutkimuksen tavoitteena on kehittää ratkaisu johonkin käytännön ongelmaan. Kasasen ym. (1991) mukaan konstruktiiviseen ongelmanratkaisuun tähtäävä normatiivinen tutkimus on mahdollista rajata innovaatiovaiheeseen ja ratkaisumallin konstruoimiseen. Tämän tutkimuksen tutkimus rajataan konstruktion innovaatiovaiheeseen:

1. Relevantin ja tutkimuksellisesti mielenkiintoisen ongelman etsiminen, joka tässä työssä on pilvipalveluiden tietosuoja.
2. Esiymmärryksen hankinta tutkimuskohteesta, joka on toteutettu tässä työssä laajalla kirjallisuuskatsauksella.
3. Innovaatiovaihe, ratkaisumallin konstruoiminen, joka tässä työssä on kerätyn aineiston analyysin perusteella muodostunut tietosuojatyön algoritmi.
4. Ratkaisun toimivuuden testaus eli konstruktion oikeellisuuden konfirmointi.
5. Ratkaisussa käytettyjen teoriakytkentöjen näyttäminen ja ratkaisun tieteellisen uutuusarvon osoittaminen.

Tutkimuksen ”innovaatiovaihe” eli ”ratkaisumallien konstruoiminen” on keskeinen tekijä uuden toimintamallin toimivuuden kannalta. Se vaatii usein heuristista ajattelua ja edellyttää tarkkaa teoreettista perustelua sekä toimivuuden testausta. Konstruktiivisen tutkimusprosessin onnistumisen kannalta innovaatiovaihe on siis ratkaisevassa asemassa. Halonen on esittänyt työssään kolme ensimmäistä vaihetta, perustuen tutkimusekonimisiin syihin. Myöskään tässä tutkimuksessa ei mallin toimivuutta testata tutkimusekonomisista syistä, joista mainittakoon muun muassa henkilövaihdokset, aikatauluin liittyvät haasteet sekö tiedonkulun vaikeudet. Konstruktion oikeellisuuden osoittaminen todennetaan myöhemmin tästä työstä mahdollisesti syntyvästä jatkotutkimuksesta. Syntynyttä konstruktiota on jo alettu testaamaan osana Valtorin tietosuojatyötä samalla kun mallin sisältöä rikastetaan Julkri kriteeristön tietosuojakontrolleilla (Valtiovarainministeriö 2023).

Konstruktiivinen tutkimusote pyrkii ratkomaan tosielämän ongelmia, joka perustuu pragmatistiseen filosofiaan. Sillä pyritään tuottamaan merkittäviä teoreettisia panoksia innovatiivisten konstruktioitten luomiseen, joilla pyritään ratkaisemaan reaalimaailman ongelmia sekä kehittämään sitä toimintaympäristöä, johon sitä sovelletaan. Sille on myös luonteenomaista, että tutkijan empiirinen interventio on eksplisiittistä ja on huolellisesti kytketty olemassa olevaan teoreettiseen tietämykseen, joka tuottaa innovatiivisen konstruktion ratkaisemaan tosielämän ongelmia. Konstruktiivisen tutkimusotteen ydinpiirteet edellyttävät, että se keskittyy tosielämän ongelmiin, jotka koetaan käytännössä tarpeellisiksi (Lukka 2006). Konstruktiivista tutkimusta voidaan tarkastella yhtenä tapaustutkimuksen muotona (Siikaniemi, 2005). Konstruktiivinen tutkimus tuo vaihtoehdon, joka soveltaa voimakasta ongelmanratkaisuun tähtäävää interventiota ja intensiivistä yritystä tehdä teoreettisia johtopäätöksiä empiiriseen työhön perustuen (ks. Lukka 2006).

Konstruktiivinen tutkimus soveltuu erityisesti ongelmanratkaisuun tähtääviin interventioihin. Konstruktiivisessa tutkimuksessa tutkijan rooli on

interventionistisempi verrattuna toiminta-analyyttisiin lähestymistapoihin, joka jakaa yhtäläisyyksiä konstruktiivisen tutkimusotteen kanssa. Toiminta-analyyttiset tutkimukset keskittyvät empiiristen ilmiöiden kuvaamiseen ilman normatiivisia tavoitteita, kun taas konstruktiivisissa tutkimuksissa ongelmanratkaisu on keskeistä (Neilimo & Näsi 1980).

Konstruktiivinen tutkimusote tarjoaa mahdollisuuksia tuottaa selkeitä käytännön hyötyjä organisaatioille. Se ideaalitapauksessa vähentää käytännön ja tutkimuksen välistä kuilua ja mahdollistaa tietämyksen ja ideoiden vaihdon. Kuitenkin tutkijan on perusteltava valittu tutkimusote ja osoitettava kontribuutionsa akateemiselle yleisölle. Onkin tärkeää analysoida perusteellisesti tutkimusongelman käytännön merkitys yhdessä kohdeorganisaation edustajien kanssa ennen tutkimuksen aloittamista. Tietosuoja-aspekteihin liittyvät huolenaiheet tuli tässä tutkimuksessa ottaa erityisesti huomioon, jolloin tutkijan oli oltava valmistautunut perustelemaan tutkimusotteen soveltuvuus tutkimusasetelmaan. Soveltuvuutta perustellaan sillä, että konstruktiivinen tutkimusote tarjoaa mahdollisuuden luoda innovatiivisia ratkaisuja reaalimaailman ongelmiin ja edistää tieteenalaa. Se vaatii tarkkaa suunnittelua ja yhteistyötä kohdeorganisaation kanssa, mutta tarjoaa mahdollisuuden merkittävään teoreettiseen kontribuutioon.

Konstruktiivinen tapaustutkimus yhdistää konstruktiivisen tutkimuksen piirteitä tapaustutkimuksen kautta tapahtuvaan monimutkaisten ilmiöiden ymmärtämiseen (Kasanen ym. 1991). Aho (2011) toteaa väitöskirjassaan konstruktiivisen tapaustutkimuksen olevan luonteva tutkimusote hänen väitöstutkimukseensa, sillä hänen tutkimuksensa ensisijainen kysymys pyrkii vastaamaan, miten suorituskyvyn johtamisen kypsyyttä voidaan arvioida organisaatiossa. Tarkoituksena on selittää ja toisaalta myös ymmärtää monimutkainen ilmiö paremmin. Vahvan intervention ja osallistuvan havainnoinnin kautta pyritään luomaan konstruktio, sekä mahdollisuuksien mukaan testaamaan sen käytettävyyttä. Kun perinteisin tapaustutkimuksen piirteisiin lisätään konstruktiivisen tutkimusotteen piirteitä ja ominaisuuksia, korostuu väitöskirjatutkimuksessa selkeämmin pragmatismi sekä tutkijan interventionistinen rooli (Aho 2011).

Kuten Ahon (2011) väitöskirjatyössä, myös tässä tutkimuksessa näitä eri otteita tarkastellaan yhtenä tutkimusotteellisena kokonaisuutena, jossa sekä tapaustutkimus, että konstruktiivinen tutkimus tukevat toinen toisiaan (Soininen 2021).

Oman, kokemuksen kautta syntyneen hiljaisen tiedon sekä aiemmin aiheesta tehdyn tutkimuksen perusteella olen kyennyt yleisellä tasolla hahmottamaan tietojärjestelmätieteen kentän uutta ilmiötä ja siihen liittyvää tutkimusongelmaa, joka on syntynyt tietosuoja-asetuksen keskeisen vaatimuksen eli sisäänrakennetun ja oletusarvoisen tietosuojan soveltamisesta pilvipalveluissa.

Jotta tutkimuskysymyksiin vastaamista varten saadaan riittävän monipuolista tietoa, tutkimus toteutettiin kaksivaiheisesti. Ensimmäinen, määrällisellä tutkimusmenetelmällä toteutettu tutkimus on **ryhmäeroja selittävä tutkimus**, joka kohdistuu kohdeorganisaation eri johtotasojen välisiin eroihin. Ryhmäeroja vertailevassa tutkimuksessa mitataan kohdeorganisaation eri johtotasojen näkemyksiä tietosuojaan liittyvistä väittämistä, jonka avulla saadaan selville ryhmien

yhtäläisyyksiä ja eroja sekä pyritään selvittämään niiden syitä. Tutkimalla korrelaatioita pyritään löytämään ilmiöiden välisiä yhteyksiä koko kohdejoukossa, jolloin mitattavien muuttujien joukkoon otetaan selittäviä muuttujia. (Eriksson & Koistinen 2014; Kekkonen 2008.)

Tuloksia varmennetaan laadullisella tutkimusmetodilla, jossa haastatellaan kuutta suomalaista tietosuoja-asiantuntijaa sekä ryhmähaastatteluna asiantuntijaryhmää yhdestä ICT-palveluntarjoajaorganisaatiosta. Haastattelukysymykset perustuvat ensimmäisen, määrällisen, tutkimuksen tuloksiin. Haastateltavien kommentit edustavat heidän omia näkemyksiään, eivätkä ne ole heidän edustamansa organisaation virallisia kantoja. Tämän triangulaatiomenetelmän tarkoituksena on verifioida tutkimuksen tuloksia, jolla vahvistetaan kahden eri tutkimuksen tulosten luotettavuutta. Soinisen (2021) tulkinnan mukaan triangulaatio tapaustutkimuksessa tarkoittaa laadullisen ja määrällisen aineiston yhdistämistä samaan tutkimukseen. Aineiston yhdistämisellä varmistetaan tulosten yhdenmukaisuus ja samansuuntaisuus, koska jokaisella metodologialla on omat heikkoutensa ja vahvuutensa (Deacon ym. 1998; Metsämuuronen 2006; Creswell & Clark 2011; Freshwater & Cahill 2013.)

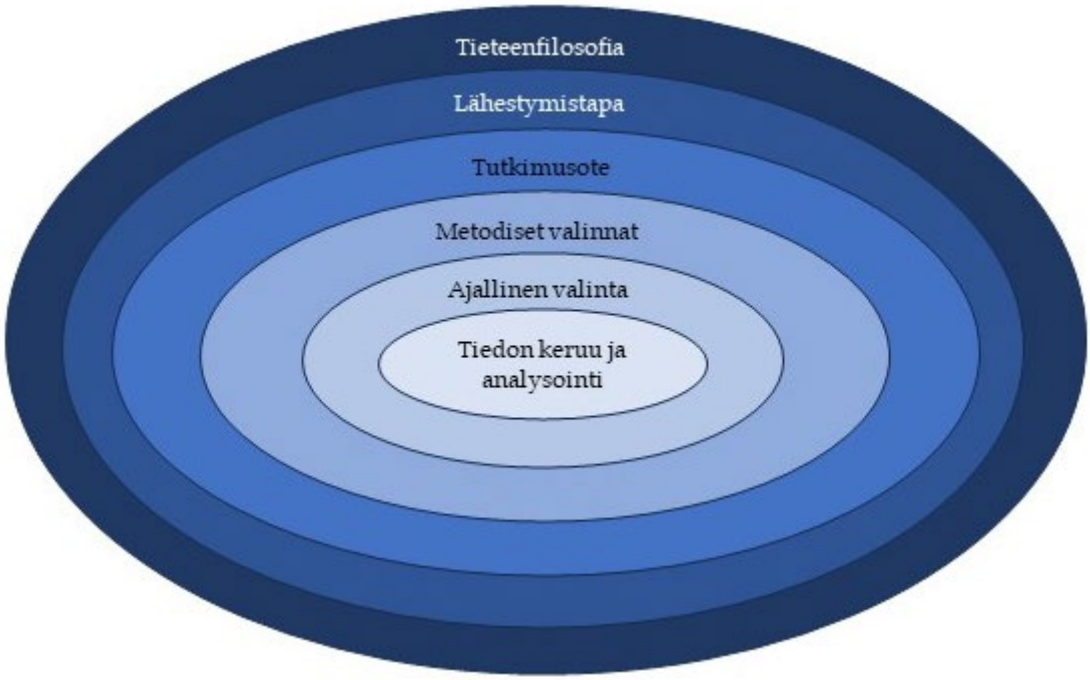
Ensimmäisenä vaiheena oli siis määrällinen tutkimus, jossa 46 henkilöä Valtorin eri johtotasoista (strateginen johto, keskijohto, lähijohto) vastasi kyselytutkimuksen väitteisiin viisiportaisesti (samaa mieltä – eri mieltä). Toisen vaiheen laadullinen tutkimus koostui kahdentyyppisistä haastatteluista: kuudesta yksilöhaastattelusta sekä yhdestä neljän hengen ryhmähaastattelusta. Haastateltavat olivat muualla kuin Valtorissa työskenteleviä tietosuoja ja -turva-asiantuntijoita. Heitä pyydettiin arvioimaan sekä ensimmäisen vaiheen tutkimustuloksia että oman organisaationsa tietosuojan kypsyystasoa.

5.1 Tutkimusmalli ja tutkimuksen toteutus

Alaluvuissa kuvataan kummankin tutkimusvaiheen yleinen tutkimusote, tutkimusmalli ja metodologia. Alaluvussa 5.3 kuvataan määrällisen tutkimuksen aineistonkeruu ja kohderyhmä sekä laadullisen tutkimuksen aineistonkeruu ja kohderyhmä.

Tutkimuksessa hyödynnetään Saundersin, Lewisin ja Thornhillin (2009) kehämäistä tutkimusmallia eli sipulimallia (kuvio 9), jossa työtä kuljetetaan tekniikan valinnan ja tiedon käsittelytapojen kautta ilmiön tarkasteluun valitussa aikaikkunassa. Sipulimalli sisältää kuusi kerrosta. Sisin kerros sisältää datan keräämisen ja analysoinnin. Toisessa kerroksessa määritellään, onko tutkimukseen kerätty aineisto kertaluonteinen vai kerätäänkö aineistoa samasta ilmiöstä useamman kerran. Kolmannessa kerroksessa valitaan tutkimuksessa käytettävä menetelmä kolmesta vaihtoehdosta. Ensimmäinen valinta tapahtuu määrällisen tai laadullisen menetelmän välillä, jolloin tutkimuksessa käytetään jompaakumpaa menetelmää. Toisessa vaihtoehdossa yhdistetään edellä mainitut menetelmät, ja kolmannessa vaihtoehdossa voidaan esimerkiksi edellisen lisäksi luokitella ja kvantifioida laadullinen aineisto tarkoituksenmukaisilta osiltaan.

Sipulimallin neljäs kerros sisältää tutkimusstrategiat, joita on seitsemän: kokeellinen eli eksperimentaalinen tutkimus, survey-tutkimus, tapaustutkimus, toimintatutkimus, grounded theory -tutkimus, etnografia ja arkistotutkimus. Sipulimallin viidennessä kerroksessa kuvataan kaksi tutkimuksen lähestymistapaa, joista ensimmäinen on induktio eli aineistolähtöinen analyysi ja toinen on deduktiivinen eli teorialähtöinen analyysi. Sipulimallin uloin eli kuudes kerros sisältää neljä tieteenfilosofista suuntausta, jotka ovat positivismi, realismi, interpretivismi ja pragmatismi.



KUVIO 9. Saundersin sipulimalli Saundersin ym. (2009) mallia soveltaen

Brymanin (2004) pragmatismikuvauksen innoittamana olen arkisessa tietosuojatyössäni ajautunut aitoon epäilyyn, ettei sisäänrakennetun ja oletusarvoisen tietosuojan vaatimuksia ole kaikilta osin tunnistettu tai juurrutettu arjen tietosuojatyöhön. Tämä epäily on laukaissut liikkeelle tämän tutkimuksen. Bryman väittää totuuden olevan jotain, jonka kaikki tietävät. Hän kuitenkin pohtii, millä perusteilla voidaan erottaa tosi käsitys (eli todellisuutta koskeva usko) epätodesta käsityksestä (eli sepitettä koskeva usko). Brymanin käsityksen mukaan ympäristöstä tehtyjen havaintojen ongelmana on, miten oikea, tosi käsitys pystytään erottamaan disinformaatiosta. Toden ja epätoden erottamiseen voidaan hakea apua triangulaatiosta, tieteellisen tutkimuksen metodien yhdistämisestä. (Bryman 2004.)

Tässä tutkimuksessa tukeudutaan triangulaatioon eli monitieteisiin tutkimusmenetelmiin tulosten mahdollisimman korkean validiteetin varmistamiseksi, mikä tuottaa syvällistä tietoa tutkimuksen mielenkiinnon kohteesta. Siksi tulosten pohjalta voidaankin esittää kysymys, onko kohdeorganisaatiosta kerätyn aineiston analyysien tulokset yleistettävissä laajemmin

valtionhallintoon. Saatuja tuloksia voitaneen käyttää katalysaattorina mahdollisille jatkotutkimuksille.

Vaikka totuuden löytyminen näyttää Brymanin mukaan toivottomalta, toimintaa ohjaa kuitenkin toivo. Toivo onkin yksi pragmaattisten teorioiden peruspilari. Niissä tähdätään aina tulevaisuuteen, hyödyntäen myös mennyttä. (Bryman 2004.)

Tässä tutkimuksessa sipulimallia lähestytään aloittamalla uloimmalta kehältä, jossa on *tieteenfilosofia*. Tällä viitataan tiedon luomisen luonteeseen ja valintoihin. Tieteenfilosofia pohtii, miten saavutettuun tietoon suhtaudutaan ja kuinka sitä tarkastellaan. Tälle tutkimukselle ominaisin tieteenfilosofinen suuntaus on pragmatismi, jossa korostetaan tiedon käytännöllistä luonnetta. Pragmatismi korostaa toimintaa ja käytännön tekemistä tutkimustyössä, ongelmanratkaisussa ja tiedon tuottamisessa. Tämä lähestyminen on perusteltua etsittäessä vastausta itse tutkimuskysymykseen. (Saunders ym. 2009; Javanainen 2019, 45–37.)

Sipulimallin seuraava kehä on *lähestymistavan määrittely*. Tutkimuksen lähtökohdat huomioon ottaen tutkimusongelmaa lähestytään induktiivisen päättelyn logiikalla. Päättely etenee tunnetuista tietosuojavaatimuksista kohti uutta tapaa toteuttaa oletusarvoista ja sisäänrakennettua tietosuojaa pilvipalveluissa tiedolla johtamisen viitekehyksestä. Päättelyn logiikka noudattaa seuraavaa polkua: Työ lähtee liikkeelle yksittäisten havaintojoukkojen tarkastelusta pilvipalveluja koskevassa tietosuojatyössä valtionhallinnossa. Havaintojoukot puretaan tietosuojavaatimuksiksi, joiden toteutumista seurataan sivulla 38 kuvatun hallintamallin avulla. Päättelyketjusta muodostuu väittämiä arvioitavaksi.

Väittämien lähteinä on käytetty EU:n tietosuoja-asetusta, kansallisia tietosuojalakeja ja tietoturvastandardeja, kriteeristöjä sekä ohjeita. Väittämät on lähetetty kohdeorganisaation esihenkilöasemassa toimiville työntekijöille arvioitavaksi. Näistä arvioista kertyy tutkimukselle havaintomateriaalia, joka muodostaa perusteet johtopäätöksiä varten. Johtopäätösten tavoitteena on kuvata tiedolla johtamisen suhdetta oletusarvoisen ja sisäänrakennetun tietosuojan vaatimuksiin.

Siirryttäessä sipulimallin kolmannelle kehälle keskitytään *tutkimusotteeseen*. Tutkimusote valitaan sen mukaan, kuinka tutkimuskysymyksiin lähdetään hakemaan vastauksia. Tässä tutkimuksessa käytetään tapaustutkimusta, joka on määritelty empiiriseksi tutkimukseksi. Tapaustutkimuksen ja sitä seuraavan triangulaation katsotaan sopivan aiheisiin, joista on tehty vain vähän empiiristä tutkimusta tai jotka ovat tässä ajassa vaikuttavia ilmiöitä. (Eriksson & Koistinen 2014.) Tässä tapauksessa kohteena on ajankohtainen ja laajavaikutteinen ilmiö, eikä aihealueesta ole kuvatusta viitekehyksestä tehty juurikaan tutkimusta.

Tapaustutkimuksille on tyypillistä, että tutkitaan ilmiöitä, jotka määräytyvät ajan, paikan tai jonkin muun kriteerin mukaan, esimerkkeinä organisaatio ja ryhmä (Yin 1983, 23; Metsämuuronen 2006). Määrällisen aineiston analyysi verifioidaan triangulaatiolla alistamalla se ulkopuolisten tietosuoja-asiantuntijoiden arvioitavaksi.

Metodologiana käytetään monimetodista tutkimusta, jossa määrällisen ja laadullisen tutkimuksen piirteitä yhdistellään triangulaation menetelmin. Määrällinen tutkimus on luonteeltaan numeerista tarkastelua, laadullinen tutkimus puolestaan ei-numeerista tutkimusta, jossa esimerkiksi haastateltavan sanallisia vastauksia tutkitaan tarkasti. Samoin otanta on yleensä pienempi kuin määrällisessä tutkimuksessa. (Saunders ym. 2009.)

Seuraavalla kehällä määritellään tutkimuksen **aikahorisontti**. Saunders ym. (2009) esittävät kaksi vaihtoehtoa, pitkittäisen ja poikkileikkaustutkimuksen. Poikkileikkaus on verrattavissa tiettynä ajankohtana otettuun valokuvaan, kun taas pitkittäinen ajanjakso tarkoittaa useasta kuvasta tehtyä sarjaa. Tätä tutkimusta voidaan pitää pitkittäistutkimuksena, koska tutkittavaa ilmiötä tarkasteltiin vuosina 2019–2022, jolloin senaikuiset tapahtumat vaikuttivat poikkeuksellisen merkittävästi tutkittavaan ilmiöön (Privacy Shield -järjestelyn kumoaminen ja esimerkiksi Vastaamon tietovuoto). Ensimmäisessä vaiheessa (2019) toteutettiin määrällinen tutkimus, jonka perusteella laadittiin laadulliset kysymykset täsmentämään määrällisen aineiston tuloksia. Tämän lisäksi toteutettiin erillinen ryhmähaastattelu vuonna 2022 valtionhallinnossa toimivien tietosuoja-asiantuntijoiden ja pilviteknologiatoimittajien näkökulman huomioimiseksi.

Tässä tutkimuksessa sipulimallin ytimessä, *aineiston keruussa,* käytetään kokonaisotantaa. Tämä tarkoittaa, että määrällisen tutkimuksen vaiheeseen otetaan mukaan koko määritelty perusjoukko eli kaikki Valtorin kolmessa eri johtotasossa toimivat henkilöt. Heikkilä (2014) toteaa, että kokonaisotanta kannattaa tehdä silloin, kun otoskooksi tulisi yli puolet perusjoukosta. Sitä kannattaa hänen mukaansa harkita myös silloin, jos yksi kolmasosa perusjoukosta tulisi otokseen. Kokonaisotantaa käytetään tavallisesti pienissä tutkimusaineistoissa, joissa on noin sata havaintoyksikköä. (Heikkilä 2014, 43.)

5.2 Tutkimuksen metodologia

Ryhmäeroja vertailevassa tutkimuksessa mitattiin kohdeorganisaation eri johtotasojen näkemyksiä tietosuojaan liittyvistä väittämistä, jotta saatiin selville ryhmien yhtäläisyyksiä ja eroja sekä selvitettiin niiden syitä. Toinen osa oli **korrelaatiotutkimus**, jossa haettiin ilmiöiden välisiä korrelaatioita tutkimalla kohdejoukkoa – sekä tutkimuskyselyn vastaajien vastauksia että haastateltavien näkemyksiä – kokonaisuutena, ja tällöin mitattavien muuttujien joukkoon otetaan selittäviä muuttujia.

Vertailevaa tutkimusta suunniteltaessa tulee tarkkaan tuoda esille, mitä tutkimuskohteesta halutaan nimenomaan saada selville. Lisäksi on mietittävä, keitä koehenkilöitä vertailuun tulee ottaa mukaan, jotta tutkimuksen tavoitteet saavutetaan. Yleisesti ottaen vertailevat tutkimukset voidaan jakaa tutkimustavoitteiden mukaan teoriaa testaaviin, teoriaa kehittäviin ja kuvaileviin tutkimuksiin. (Eriksson & Koistinen 2014.)

Vertailevassa tutkimuksessa on vaarana, että kontrolli voi jäädä puutteelliseksi (Kekkonen 2008). Tässä työssä kyseistä mahdollisuutta hallitaan

verifioimalla saatu tulos triangulaatiolla: ryhmäerojen tuloksia joko vahvistetaan tai kyseenalaistetaan laadullisen tutkimuksen tuloksilla.

Tutkimuksessa on hyväksyttävä muuttujiin liittyvä luonnollinen vaihtelu, samoin kuin se, että teoreettiset lähtökohdat voivat ovat kapeammat kuin esimerkiksi kokeellisessa tutkimuksessa. Hypoteesit voivat olla joko todellisia tai ns. työhypoteeseja. Usein vertaileva tutkimus tuottaakin tutkimushypoteeseja kokeelliselle tutkimukselle. Siksi muuttujien määrä on vertailevassa tutkimuksessa usein suuri. Vertailevassa tutkimuksessa voidaan tehdä tutkimusasetelma, jossa ilmenevät muuttujat ja niiden väliset suhteet.

5.3 Tutkimusmenetelmien valinta

Soinisen mukaan (2021) määrällisen eli kvantitatiivisen tutkimuksen tarkoituksena on kuvailla, kartoittaa, verrata, selittää tai ennustaa tutkimuskohteen ominaisuuksia ja ilmiöitä (Walliman 2005, 114–115; Hirsjärvi & Hurme 2008). Näin saadaan luotua uutta teoriaa tai vahvistusta arkipäivän olettamuksiin (Walliman 2005, 105–107; Metsämuuronen 2011). Tavoitteena on kuvata tutkittavien toimintaa ja ajattelua aineistolähtöisesti. Tutkimuksen tavoite ei ole tulosten yleistettävyys vaan ilmiön ymmärtäminen siinä ympäristössä, jossa tutkittava toimii. Keskeistä on ymmärtää, että samasta ilmiöstä voi olla monia totuuksia ja että todellisuus rakentuu yksilöiden kokemuksista ja tulkinnoista. Tutkimuksen tavoitteena ei ole esittää eksplisiittistä totuutta, vaan kuvata yhtä mahdollista todellisuutta, joka perustuu tutkijan tekemiin tulkintoihin tutkimuskohteesta luovan prosessin tuloksena. (Alasuutari 2011.)

Määrällisessä tutkimuksessa esitetään perusteltuja hypoteeseja, jotka voivat perustua teoriaan tai niiden pohjalta esitettyihin malleihin. Tässä työssä mallina toimii tiedolla johtamisen hyödyntäminen siten, että sisäänrakennettu ja oletusarvoinen tietosuoja toteutuisi vaatimusten mukaisesti. Vealin (1997, 29) mukaan hypoteeseja voidaan asettaa myös kokemuksen tai havaintojen perusteella. Tapaustutkimukseen liittyvä epistemologinen kysymys voidaan esittää seuraavasti: mitä voimme oppia yhdestä tutkittavasta tapauksesta? (Metsämuuronen 2011, 222–223.)

6 SUORITETUT TUTKIMUKSET

6.1 Kyselytutkimus

Tutkimus toteutettiin hyödyntämällä kahta eri menetelmää. Aineistonkeruu aloitettiin tekemällä Valtorissa kyselytutkimus. Kohderyhmäksi valittiin ne toimihenkilöt, jotka ovat esihenkilötehtävissä (N = 106). Valtorissa esihenkilöt jaettiin tutkimuksen ajankohtana kolmeen eri luokkaan: strateginen johto, keskijohto sekä lähijohto.

Määrällinen tutkimusaineisto kerättiin strukturoidulla kyselylomakkeella. Kyselylomakkeen sisältö ja tekninen toteutus testattiin koeryhmällä (N = 7). Palautteen perusteella kysymysten sisältöä stilisoitiin ja tarkennettiin. Lisäksi varmistettiin, että kerättävä aineisto säilyy eheänä teknisessä ympäristössä.

Kysely toteutettiin marraskuussa 2020 TCD Consulting and Research Oy:n kehittämällä TCDSurvey-ohjelmistolla. Vastaajille lähetettiin kolme muistutusviestiä vastausprosentin nostamiseksi. Vastaajajoukko oli 106, ja vastaajien määrä oli 46. Vastausprosentiksi tuli 43. Vastausprosentti voidaan nähdä hyvänä huomioiden se, mitä kyberturvallisuuden hallinnan tutkimuksissa vastausprosentti tyypillisesti on. Esimerkiksi tietojärjestelmätieteen arvostetuimmassa MIS Quarterly -lehdessä julkaistun Moodyn, Siposen ja Pahnilan (2018) tutkimuksen vastausprosentti oli noin 24 %.

Vastaajat arvioivat tietosuoja-asetuksesta ja kansallisesta tietosuojalainsäädännöstä nostettuja tietosuojaväittämiä viisiportaisella Likert-asteikolla, joka on mielipideväittämissä yleisesti käytetty järjestysasteikko. Perusidea on, että asteikon keskikohdasta lähtien toiseen suuntaan samanmielisyys kasvaa ja toiseen samanmielisyys vähenee. (Heikkilä 2014, 53.) Tässä tutkimuksessa käytetään viisiportaista asteikkoa seuraavasti: 1 = olen täysin eri mieltä, 2 = olen eri mieltä, 3 = en ole samaa enkä eri mieltä, 4 = olen samaa mieltä ja 5 = olen täysin samaa mieltä. Lisäksi lomakkeessa arvioidaan väittämän merkityksellisyyttä vastaajan

omassa päätöksenteossa. Kunkin väittämän jälkeen annetaan kolme vaihtoehtoa: 1) merkityksetön, 2) ei mielipidettä ja 3) merkityksellinen. (Liite 2)

Kyselylomakkeen sisältämät tietosuojaan liittyvät väittämät on muodostettu sekä EU:n tietosuoja-asetuksen että kansallisen tietosuojalain vaatimusten ja ohjeiden pohjalta. Koska väittämät on johdettu suoraan lainsäädännöstä, on perusteltua odottaa, että väittämiin vastataan yhdenmukaisesti. Taulukossa 2 on esitetty pelkistetysti tässä tutkimuksessa käytetyt aineiston analyysimenetelmät.

TAULUKKO 2. Aineiston analyysimenetelmät

Analyysimenetelmä	**Tekijät**
Spearmanin rho-testi	Väittämien korrelaatiot
Cronbachin alpha	Aineiston reliabiliteetti
One-Sample Kolmogorov–Smirnov-testi	Summamuuttujien normaalijakautuneisuus
Crohnbachin alpha -kerroin	Summamuuttujien (faktoreiden) määrittely
Kruskall–Wallisin T-testi	Väittämien tilastollisten erojen todentaminen

Koska työssä käytettävät muuttujat ovat luonteeltaan järjestysasteikollisia, jolloin luokkien välinen etäisyys toisistaan ei ole vakio, käytettiin mediaania jakauman keskilukuna. Keskiarvo ei välttämättä antaisi rakennetussa tutkimusasetelmassa todellista kuvaa jakauman keskiluvusta. Tilastollisella merkitsevyydellä tuodaan esille, kuinka todennäköisesti tutkimuksen tulokset ovat todellisia eivätkä sattumia. Tyypillinen tilastollisen merkitsevyyden raja-arvo (p-arvo) on 0,05, joka kuvaa todennäköisyyttä saada saatu tulos uudestaan, mikäli tutkimuksen nollahypoteesi pitää paikkansa. Mikäli testin tulos jää alle 0,05:n, voidaan olettaa, että ryhmien välisen eron taustalla sattuman todennäköisyys on alle 5 %.

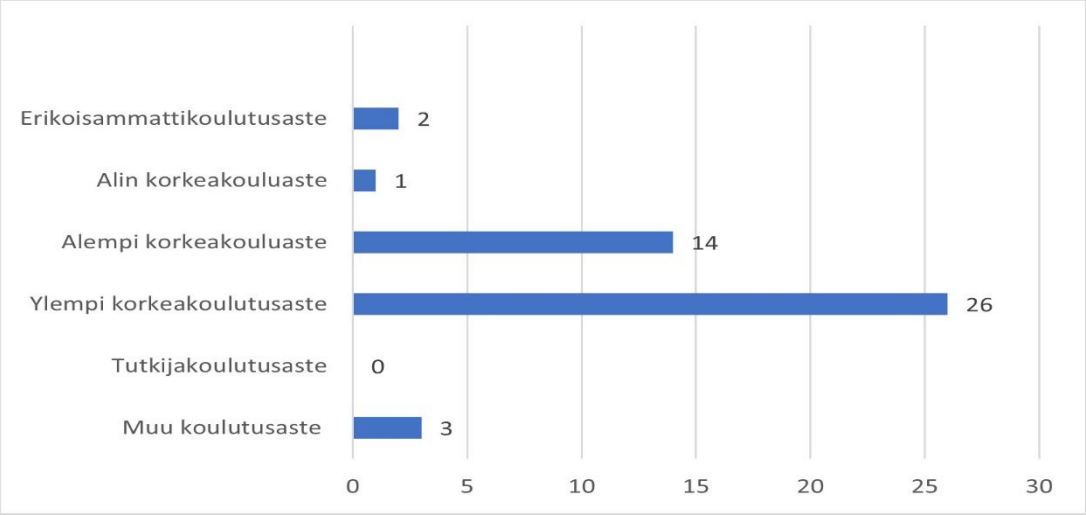
Mikäli testin tulos on 0, ei kahden muuttujan välillä ole tilastollista yhteyttä. Mitä lähempänä testin tulos on 1:tä tai -1:tä (täydellinen korrelaatio), sitä vahvempi yhteys muuttujien välillä on. Lähempänä 1:tä oleva tulos viittaa suoraan verrannolliseen yhteyteen, ja lähempänä -1:tä oleva tulos viittaa kääntäen verrannolliseen yhteyteen. Spearmanin järjestyskorrelaatiokerroin on Pearsonin korrelaatiokertoimen erityistapaus. Spearmanin järjestyskorrelaatiossa mitattavien muuttujien arvot on korvattu järjestysluvuilla. Spearmanin järjestyskorrelaatio ei reagoi parametrien poikkeamiin lineaarisuudesta yhtä voimakkaasti kuin Pearsonin korrelaatiotesti, koska Spearmanin järjestyskorrelaatio mittaa kahden satunnaismuuttujan välistä monotonista riippuvuutta. Jos muuttujan hajonta on pieni, molemmat korrelaatioanalyysit antavat lähes samanlaiset arvot.

Tilastollinen merkitsevyys ei kuitenkaan anna yksiselitteitä tietoa vaikuttavuudesta, joka tässä työssä tarkoittaisi, että tutkittavana olevaa asiaa todella hyödynnettäisiin oletusarvoisen ja sisäänrakennetun tietosuojan jalkauttamisessa valtionhallintoon.

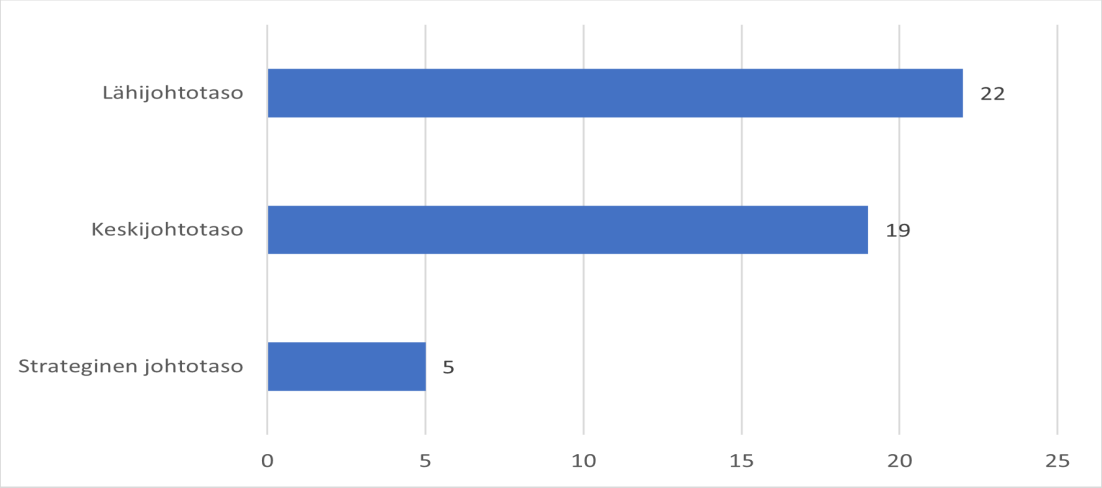
6.1.1 Taustatiedot

Tutkimukseen osallistuneista kerättiin seuraavat, aiheen kannalta merkittäviksi ajatellut taustatiedot: koulutusaste, esihenkilötaso, toimintayksikkö, arvio henkilötietojen käsittelyn määrästä ja arvio omasta tietosuojaosaamisesta.

Kaikkiaan 46 vastaajasta 26 on suorittanut ylemmän korkeakoulututkinnon. Pienin edustus on alimman korkeakouluasteen suorittaneilla. (Kuvio 10.) Kuviossa 11 esitetään vastaajien jakautuminen kolmeen esihenkilötasoon: strategiseen johtoon, keskijohtoon ja lähijohtoon. Eri johtotasot olivat tasapainoisesti edustettuina sen mukaisesti, mikä on koko organisaation johtamismalli tutkimuksen tekohetkellä.



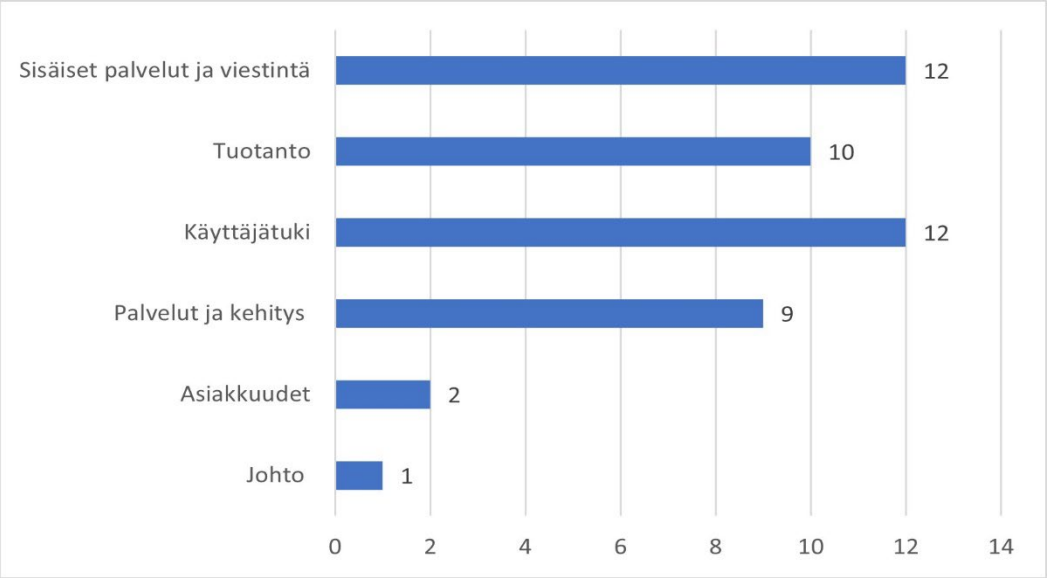
KUVIO 10. Vastaajien koulutusaste



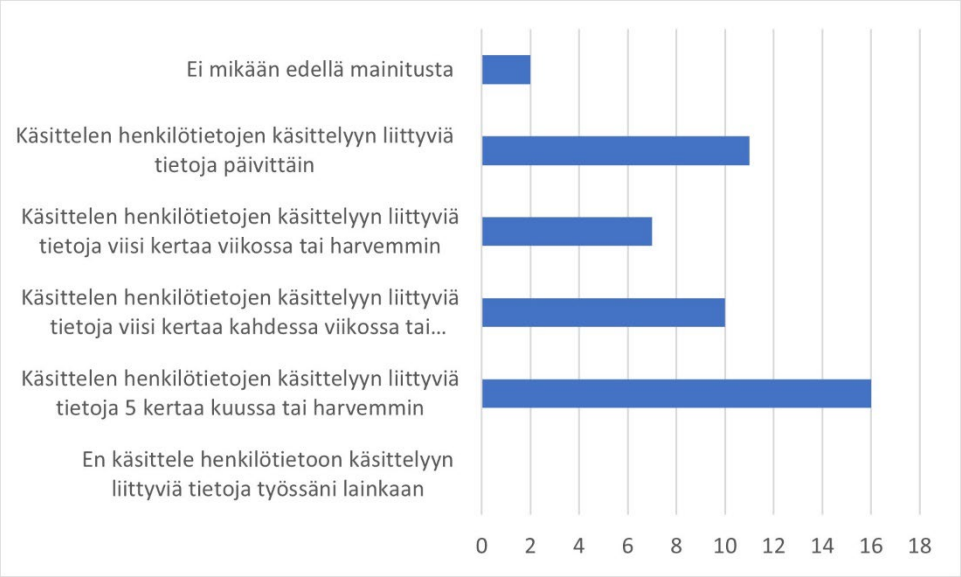
KUVIO 11. Vastaajien esihenkilötaso Valtorissa

Suurin osa vastaajista tulee Valtorin tuotannosta, sisäisistä palveluista, käyttäjätuesta sekä palvelut ja kehitys -yksiköstä. Henkilötietojen käsittely on keskittynyt selkeästi näihin yksiköihin. Oletusarvoisen ja sisäänrakennetun tietosuojan kehittäminen tulee aloittaa juuri niistä, sillä niistä käsin toimintamallit ovat juurrutettavissa toisiin yksiköihin. Kuviossa 12 kuvataan, missä toimintayksikössä vastaajat työskentelivät.

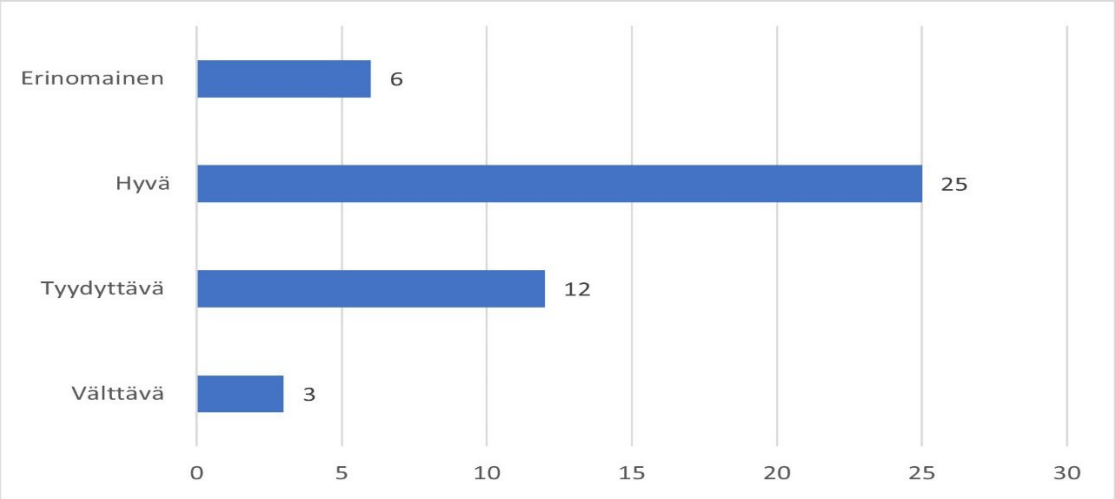
Henkilötietojen käsittely on yleistä kohdeorganisaation kaikilla johtotasoilla. Kuvio 13 osoittaa, kuinka usein vastaajat oman ilmoituksensa mukaan käsittelevät työssään tietosuojaan liittyviä kysymyksiä.



KUVIO 12. Vastaajien toimintayksiköt



KUVIO 13. Henkilötietojen käsittelyn määrä omassa työssä



KUVIO 14. Vastaajien arvio omasta tietosuojaosaamisestaan

Vastaajat arvioivat yleisellä tasolla omaa tietosuojaosaamistaan (kuvio 14). Yli puolet vastaajista piti tietosuojaosaamistaan joko hyvänä tai erinomaisena.

Merkittävällä osalla vastaajista on siis alempi tai ylempi korkeakoulututkinto (86 %), ja suurin osa vastaajista tulee Valtorin tuotannosta, sisäisistä palveluista, käyttäjätuesta sekä palvelut ja kehitys -yksiköstä. Näissä yksiköissä käsitellään merkittävässä määrin henkilötietoja niin rekisterinpitäjän kun tietojenkäsittelijän rooleissa. Henkilötietojen käsittely on yleistä kaikilla johtotasoilla. Yli puolet vastaajista pitää tietosuojaosaamistaan joko hyvänä tai erinomaisena. Vastaus on ristiriidassa väittämien vastausten suuren hajonnan kanssa. Mikäli tietosuojaosaaminen olisi hyvää tai erinomaista, väitteisiin vastattaisiin yhtenäisesti. Myöskään koulutustaso ei korreloinut tietosuojaosaamisen kanssa.

6.1.2 Vastaukset väittämittäin

Väittämät liittyvät tietosuojan hallintamallin kaikkiin viiteen osa-alueeseen (hallinnollinen tietosuoja, operatiivinen tietosuoja, tietosuojariskien hallinta, tietosuojan ja tietoturvan välinen kytkös eli vuorovaikutus sekä sisäänrakennettu ja oletusarvoinen tietosuoja), ja tutkimuksessa väittämiä tarkastellaan myös hallintamallin osa-alueiden mukaisissa ryhmissä. (Väittämät ovat nähtävissä osa-alueittain järjestettyinä liitteessä 1.)

Väittämät, joiden kanssa vastaajat ovat eri mieltä tai täysin eri mieltä (keskiarvot joko ≤ 2,50 tai ≥ 3,75), ovat

1. Ennen pilvipalveluiden käyttöönottoa voin hyödyntää näyttöön perustuvaa tietoa arvioidakseni, siirtyvätkö pilvipalveluihin kerätyt henkilötiedot EU alueen ulkopuolelle.
2. Olen saanut tarpeeksi informaatiota EU:n mallisopimuslausekkeiden hyödyntämisestä.
3. Olen saanut tarpeeksi informaatiota Privacy Shield -järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyssä.

4. Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa käsiteltävien erityisten (arkaluonteiset) henkilötietojen käsittelyn vaatimustenmukaisuuden.
5. Valtorin ylimmällä johdolla on kokonaisvastuu vaatimusten mukaisen tietosuojan toteuttamiseksi.
6. Saan riittävästi informaatiota tietosuojan jäännösriskien arviointia varten ennen pilvipalvelun käyttöönottoa.
7. Valtorissa on henkilötietojen käsittely kuvattuna tietovirta kaaviona.
8. Tietosuojan vaikutusten arviointi on minulle käsitteenä tuttu.
9. Saan riittävästi informaatiota pilvipalveluiden kriisinkestävyyden arviointia varten tietosuojan viitekehyksestä.
10. Saan riittävästi informaatiota pilvipalveluiden pääsynhallintaan liittyvien kysymysten arviointia varten tietosuojan viitekehyksestä.
11. Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa tapahtuvan henkilötietojen pseudonymisoinnin tarpeen.
12. Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluiden varmuuskopioiden ja lokien vaatimustenmukaisuuden.
13. Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa tapahtuvan henkilötietojen säilytyksen vaatimustenmukaisuuden.
14. Saan riittävästi informaatiota, jotta voin arvioida, miten turvallista pilvipalveluissa tapahtuva henkilötietojen käsittely on. Väittämässä viitataan henkilötietojen siirtoon eri maantieteellisten alueiden välillä.
15. Tunnen Valtorin henkilötietojen luovutusten prosessin.
16. Käytettäessä pilvipalveluita osoitetaan Valtorissa näyttöön perustuen, että henkilötietojen minimikäsittelyn vaatimukset toteutuvat.
17. Saan tarpeeksi informaatiota tarkoituksenmukaisen henkilötiedonkäsittelyn määrittelemiseksi pilvipalveluissa
18. Tiedän keneltä kysyä tietosuojaan liittyvää informaatiota Valtorissa

Väitteet perustuvat voimassa olevaan lainsäädäntöön, ja siksi vastaajien tulisi olla väittämien kanssa vähintään samaa mieltä, mieluiten täysin samaa mieltä (väittämien asteikko on 1 = täysin eri mieltä, 2 = eri mieltä, 3 = ei eri eikä samaa mieltä, 4 = samaa mieltä ja 5 = täysin samaa mieltä). Silloin rekisteröityjen oikeuksien voitaisiin katsoa toteutuvan.

Seuraavaksi käydään läpi nämä väittämät, joiden kanssa vastaajat ovat eri mieltä tai täysin eri mieltä:

Ennen pilvipalveluiden käyttöönottoa voin hyödyntää näyttöön perustuvaa tietoa arvioidakseni, siirtyvätkö pilvipalveluihin kerätyt henkilötiedot EU-alueen ulkopuolelle. Jos henkilötietoja siirtyy Euroopan unionin tai Euroopan talousalueen ulkopuolelle kolmansiin maihin, rekisterinpitäjän on varmistettava, onko siiroille hyväksytty peruste, joka vastaa sekä käyttösidonnaisuuden periaatteita että tietoturvan teknisiä vaatimuksia. EU:n alueen ulkopuolelle tapahtuvan henkilötietojen siirron oikeusperustana on oltava sopimus, joka turvaa asianmukaisen tietosuojan tason. Sopimuksessa on oltava riittäviä turvatoimia kuvattuna, ja sopimuksen on oltava sitova. EU:n alueen ulkopuolella olevassa yrityksessä henkilötietoja käsittelyn tulee olla EU:n tietosuoja-asetuksen

vaatimusten mukaista ja käsittelijällä on osoitusvelvollisuus vaatimustenmukaisuudesta. Esille tulee kuitenkin kritiikkiä siitä, ettei pilvipalveluiden toimittajien toiminta ole tältä osin aina läpinäkyvää. Vastausten keskiarvo on 2,25 ja mediaani 2,00. Keskihajonta on 0,92, eli vastaajat arvioivat väittämää hieman eri tavoilla. Tulokset osoittavat, ettei Valtorissa ennen pilvipalveluiden käyttöönottoa hyödynnetä näyttöön perustuvaa tietoa arvioitaessa, siirtyvätkö pilvipalveluihin kerätyt henkilötiedot EU-alueen ulkopuolelle.

Olen saanut tarpeeksi informaatiota EU:n mallisopimuslausekkeiden hyödyntämisestä. EU:n mallisopimuslausekkeiden avulla henkilötietoja voidaan hyväksyttävästi siirtää EU:n ja ETA:n ulkopuolelle. Vastausten keskiarvo on 2,04 ja mediaani 1,90. Vastausten keskihajonta on 0,90. Tuloksen perusteella voidaan todeta, ettei Valtorissa saada tarpeeksi informaatiota EU:n mallisopimuslausekkeiden hyödyntämisestä tai sitä ei esitetä ymmärrettävästi eri johtotasoille.

Olen saanut tarpeeksi informaatiota Privacy Shield -järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyssä. Privacy Shield -sopimuksen tarkoituksena oli varmistaa, että eurooppalaisten henkilötietoja suojataan, kun niitä siirretään kaupallisessa tarkoituksessa EU:n alueelta Yhdysvaltoihin, mutta sopimus kumottiin vuonna 2020. Informaatiolla tarkoitetaan mitä tahansa tietoa, jonka avulla voidaan arvioida Privacy Shield -sopimuksen mitätöimisen vaikutuksia rekisteröidyn oikeuksiin. Vastausten keskiarvo on 2,24 ja mediaani on 2,00. Vastausten keskihajonta on 1,17, joka ilmaisee vastaajien arvioivan väittämää eri tavalla. Tulokset osoittavat, ettei Valtorissa ole riittävästi informaatiota Privacy Shield -järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyyn tai informaatio ei ole ymmärrettävää organisaation eri johtotasoilla.

Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa käsiteltävien erityisten (arkaluonteiset) henkilötietojen käsittelyn vaatimustenmukaisuuden. Pilvipalveluissa käsiteltävillä erityisillä henkilötiedoilla tarkoitetaan EU:n tietosuoja-asetuksen artiklan 9 mukaan rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista tai filosofista vakaumusta, ammattiliiton jäsenyyttä, geneettisiä ja biometrisiä tietoja, terveyttä koskevia tietoja sekä seksuaalista käyttäytymistä ja suuntautumista. Vaatimuksenmukaisuudella tarkoitetaan edellä kuvattujen tietojen tietoturvan vaatimusten toteutumista. Vastausten keskiarvo on 2,23 ja mediaani on 2,00. Vastauksissa on pientä hajontaa; keskihajonta on 0,94. Tulokset osoittavat, ettei Valtorissa ole riittävästi informaatiota, jotta erityisten henkilötietojen käsittelyn vaatimustenmukaisuutta kyettäisiin arvioimaan tai informaatio ei ole ymmärrettävää organisaation eri johtotasoilla.

Valtorin ylimmällä johdolla on kokonaisvastuu vaatimusten mukaisen tietosuojan toteuttamiseksi. Vastausten keskiarvo on 4,46 ja mediaani on 4,90. Vastaajat arvioivat väittämää hieman eri tavalla, ja keskihajonta on 0,76. Tulokset osoittavat, että tietosuojan kokonaisvastuu on tunnistettu asetuksen vaatimusten mukaisesti.

Saan riittävästi informaatiota tietosuojan jäännösriskien arviointia varten ennen pilvipalvelun käyttöönottoa. Jäännösriskillä tarkoitetaan sellaista riskiä, joka on tunnistettu vaikutustenarvioinnin aikana. Kun jäännösriski on

tunnistettu, on tarkoituksenmukaista joko poistaa riski kokonaan tai, joissain tapauksissa, organisaation ylimmän johdon hyväksynnän jälkeen hyväksyä tunnistettujen jäännösriskien mitigointikeinot. Vastausten keskiarvo on 2,33 ja mediaani on 2,22. Informaatiolla tarkoitetaan tässä selkeitä raportteja, jotka tukevat johdon jäännösriskeistä tekemiä linjauksia. Tulosten perusteella voidaan arvioida, etteivät Valtorin eri johtotasot saa riittävästi informaatiota tietosuojan jäännösriskien arviointia varten ennen pilvipalvelun käyttöönottoa.

Valtorissa on henkilötietojen käsittely kuvattuna tietovirtakaaviona. Tietovirtakaaviolla kuvataan henkilötietojen siirtymistä rekistereistä eri tietojärjestelmiin. Kaavio auttaa hahmottamaan tiedonkäsittelyn käyttösidonnaisuuden, minimikäsittelyn vaatimukset sekä elinkaaren hallinnan. Vastausten keskiarvo on 2,24 ja mediaani on 2,20. Vastaajat arvioivat väittämää hieman eri tavalla, ja keskihajonta on 0,94. Tulokset osoittavat, ettei henkilötietoja ole Valtorissa vaaditulla tasolla kuvattu tietovirtakaaviona.

Tietosuojan vaikutusten arviointi on minulle käsitteenä tuttu. Väitteen vastausten keskiarvo on 3,50. Vastaajat ovat väittämän kanssa samaa mieltä, joskin hajontaa on havaittavissa; keskihajonta on 0,91.

Saan riittävästi informaatiota pilvipalveluiden kriisinkestävyyden arviointia varten tietosuojan viitekehyksestä. Pilvipalveluiden kriisinkestävyydellä tarkoitetaan palveluiden kykyä sietää poikkeamatilanteita sekä palautua niistä. Informaatiolla tarkoitetaan tässä selkeitä ohjeita ja linjauksia, joilla tuetaan kriisinkestävyyttä. Vastausten keskiarvo on 2,18 ja mediaani on 2,00. Vastausten keskihajonta on 0,85. Vastaajat ovat eri mieltä tämän väittämän kanssa. Tulokset osoittavat, ettei Valtorissa ole selkeitä ohjeita ja linjauksia, joilla tuetaan kriisinkestävyyttä tietosuojan viitekehyksestä.

Saan riittävästi informaatiota pilvipalveluiden pääsynhallintaan liittyvien kysymysten arviointia varten tietosuojan viitekehyksestä. Pilvipalveluiden pääsynhallinnalla määritellään, osoitetaan ja hallinnoidaan organisaatioresurssien käyttöoikeuksia, myös erityyppisiin henkilötietoihin. Vastausten keskiarvo 2,17 ja mediaani on 2,00 sekä vastausten hajonta on 0,87. Vastaajat kokevat, ettei heillä ole riittävästi informaatiota pilvipalveluiden pääsynhallintaan liittyvien kysymysten arviointia varten tai sitä ei ole esitetty ymmärrettävästi eri johtotasoille.

Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa tapahtuvan henkilötietojen pseudonymisoinnin tarpeen. Pseudonymisoinnilla tarkoitetaan menetelmiä, joilla henkilötiedot käsitellään siten, ettei tietoja voi enää yhdistää tiettyyn henkilöön. Informaatiolla tarkoitetaan tässä selkeitä ohjeita ja linjauksia, jotka tukevat päätöksiä pseudonymisoinnin tarpeesta. Vastausten keskiarvo on 2,17 ja mediaani on 2,00. Vastausten keskihajonta on 0,87. Tulokset osoittavat, ettei Valtorissa ole selkeitä ohjeita ja linjauksia, jotka tukevat päätöksiä pseudonymisoinnin tarpeesta.

Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluiden varmuuskopioiden ja lokien vaatimustenmukaisuuden. Pilvipalveluiden varmuuskopioiden ja lokien vaatimustenmukaisuus todennetaan sisäisellä

tarkastuksella tai teettämällä tarkastus riippumattomalla toimijalla. Havaitut poikkeamat tulee dokumentoida, priorisoida ja korjata niiden kriittisyyden mukaisesti. Ylin johto vastaa siitä, että havaitut poikkeamat priorisoidaan ja korvaavat suojaukset tai korjaukset toteutetaan riittävän nopeasti. Vastausten keskiarvo on 2,30 ja mediaani 2,10. Vastausten keskihajonta on 0,94, joka osoittaa vastaajien arvioineen väittämää hieman eri tavalla. Tulokset osoittavat, ettei Valtorissa ole riittävästi informaatiota pilvipalveluiden varmuuskopioiden ja lokien vaatimustenmukaisuuden arviointiin.

Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa tapahtuvan henkilötietojen säilytyksen vaatimustenmukaisuuden. Henkilötietojen säilytys liittyy keskeisesti tiedon elinkaaren hallintaan, jossa määritellään tiedon olemassaolon vaiheet tiedon synnystä sen mahdolliseen hävittämiseen asti. Informaatiolla viitataan kuvaukseen tiedon elinkaaresta, jonka olemassaolo rekisterinpitäjän tulee varmistaa. Tietojenkäsittelijöillä on velvollisuus osoittaa, että tietojenkäsittely-ympäristö on vaatimustenmukainen. Vastausten keskiarvo on 2,33 ja mediaani 2,00. Vastausten keskihajonta on 1,01, joten vastaajat arvioivat väittämää eri tavalla. Tulosten perusteella voidaan todeta, etteivät Valtorin eri johtotasot saa riittävästi informaatiota, jotta he kykenisivät arvioimaan pilvipalveluissa tapahtuvan henkilötietojen säilytyksen vaatimustenmukaisuuden.

Saan riittävästi informaatiota, jotta voin arvioida, miten turvallista pilvipalveluissa tapahtuvan henkilötietojen käsittely on. Väittämässä viitataan henkilötietojen siirtoon eri maantieteellisten alueiden välillä. Henkilötietojen siirtäminen Euroopan talousalueen ulkopuolelle edellyttää erityistä siirtoperustetta. Siirrettäessä henkilötietoja EU:n ja ETA-alueen ulkopuolelle kolmansiin maihin voi rekisteröidyn oikeuksille ja vapauksille muodostua merkittävä riski, ja sen vuoksi tietosuoja-asetuksessa määritellään edellytyksiä, joilla henkilötietoja voidaan siirtää ETA-alueen ulkopuolelle. Vastausten keskiarvo on 2,30 ja mediaani on 2,00. Vastaajat arvioivat väittämää keskenään hieman eri tavalla, sillä keskihajonta on 0,99. Tulosten perusteella voidaan todeta, ettei Valtorin eri johtotasoilla ole riittävästi informaatiota, jotta voisi arvioida, miten turvallista pilvipalveluissa tapahtuva henkilötietojen siirto on. Vastausten perusteella tulee voimakkaimmin kyseenalaiseksi rekisteröityjen oikeuksien toteutuminen tietojen siirtämisessä. Siirrettäessä tietoja kolmansiin maihin, entistä kauemmaksi rekisterinpitäjästä, on ilmeinen vaara, etteivät edellä kuvatut vaatimukset toteudu. Tietojenkäsittelyn lainmukaisuutta ei voida varmistaa, koska EU-alueen ulkopuolella noudatetaan EU:n tietosuoja-asetuksesta poikkeavaa lainsäädäntöä.

Tunnen Valtorin henkilötietojen luovutusten prosessin. Valtorin henkilötietojen luovutusten prosessin mukaan on varmistauduttava siitä, että pyynnössä on mainittu luovutuksen tarkoitus ja että tietojen pyytäjällä on tosiasiallinen oikeus pyydettyihin tietoihin. Vastausten keskiarvo 2,41 ja mediaani 2,00. Vastaajien arviot väittämästä vaihtelivat, ja keskihajonta on 1,06. Tulosten perusteella voidaan todeta, etteivät vastaajat tunteneet tietojenluovutusprosessia vaaditulla tasolla.

Käytettäessä pilvipalveluita osoitetaan Valtorissa näyttöön perustuen, että henkilötietojen minimikäsittelyn vaatimukset toteutuvat. Henkilötietoja saa

käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta. Vastausten keskiarvo on 2,42 ja mediaani 2,50. Vastausten keskihajonta on 0,93, joka tarkoittaa sitä, että vastaajilla on hieman erilaisia näkemyksiä väittämästä. Tulosten perusteella voidaan todeta, ettei Valtorissa ole kypsyyttä osoittaa näyttöön perustuen, että henkilötietojen minimikäsittelyn vaatimukset toteutuvat.

Saan tarpeeksi informaatiota tarkoituksenmukaisen henkilötiedonkäsittelyn määrittelemiseksi pilvipalveluissa. Henkilötietojen käsittelyn tarkoituksenmukaisuus julkishallinnossa on todennettavissa siten, että käsittely on suunniteltu ja määritelty selkeästi rekisterinpitäjien lakisääteisten tehtävien mukaisesti. Rekisterinpitäjien lukuun toimivat tietojenkäsittelijät ovat velvollisia osoittamaan tietojenkäsittelyn vastaavan rekisterinpitäjän vaatimuksia. Vastausten keskiarvo on 2,49 ja mediaani 2,50. Vastausten keskihajonta on 1,04, joka tarkoittaa, että vastaajat arvioivat väittämää eri tavalla. Tämä tarkoittaa, että Valtorissa on heikosti käytettävissä informaatiota, jolla osoitetaan tiedon käyttösidonnaisuus.

Tiedän keneltä kysyä tietosuojaan liittyvää informaatiota Valtorissa. Väitteen vastausten keskiarvo on 4,06. Vastaajat ovat väittämän kanssa samaa mieltä, joskin hajonta on suurta; keskihajonta on 1,16.

Aineiston perusteella saa vaikutelman, että Valtorin kypsyystasoa tietosuoja-asioissa on vahvistettava. Hallintamallin osa-alueiden korrelaatiot (r) ja tilastolliset merkitsevyydet (p) on esitetty taulukossa 3. Tuloksista voidaan havaita, että väittämien väliset korrelaatiot ovat tilastollisesti merkitseviä ja suunnaltaan positiivisia. Korrelaatioiden vaihteluväli on 0,48–0,81 (.479**–.808**). Väittämien väliset tilastolliset merkitsevyydet (p-arvot) vahvistavat väittämien korrelaatiot (p = .001 tai .000). Tämä tarkoittaa sitä, että osa-alueiden (summamuuttujien) yleistäminen perusjoukkoon voidaan tehdä.

Korrelaatiokertoimen merkitsevyyden testaamiseksi laskettiin p-arvo, joka vastaa siihen, kuinka todennäköistä on saada havaitun suuruinen tai vielä kauempana nollasta oleva korrelaatiokertoimen arvo ilman että korrelaatiota on perusjoukossa. Mitä pienempi p-arvo on, sitä enemmän korrelaation yleistäminen perusjoukkoon saa tukea. Jos korrelaatio on heikko, ei muuttujien välillä ole yhteisvaihtelua. Vakiintuneen tavan mukaisesti alle 0,05:n (5 %) suuruista p-arvoa pidetään riittävänä näyttönä perusjoukossa esiintyvän korrelaation puolesta.

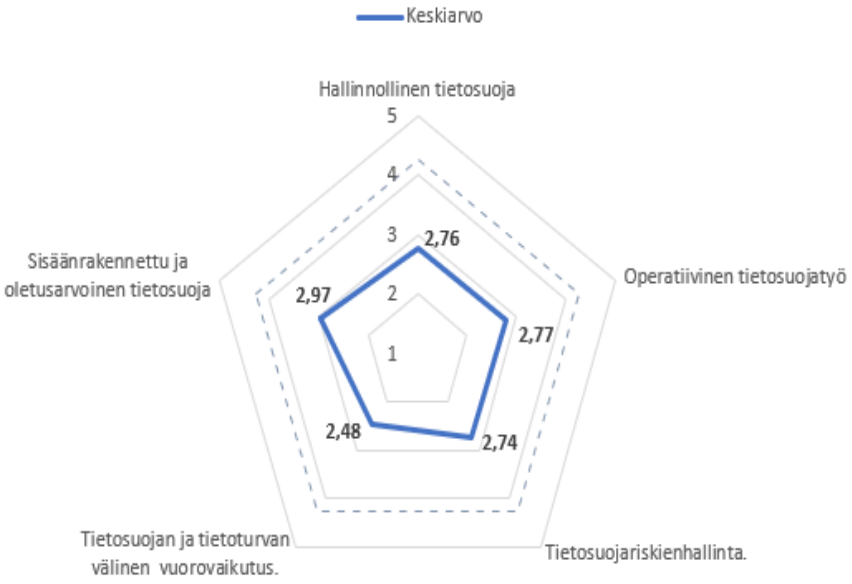
TAULUKKO 3. Valtorin tietosuojan hallintamallin korrelaatiot

Spearman's rho		Hallinnollinen tietosuoja	Operatiivinen tietosuoja	Riskiperusteinen tietosuoja	Tietosuojan ja tietoturvan välinen suhde	Sisäänrakennettu ja oletusarvoinen tietosuoja
Hallinnollinen tietosuoja	Korrelaatiokerroin	1.000	.587**	.492**	.795**	.700**
	P-arvo		.000	.000	.000	.000
	N	46	46	46	46	46
Operatiivinen tietosuoja	Korrelaatiokerroin	.578**	1.000	.479**	.660**	.559**
	P-arvo	.000		.001	.000	.000
	N	46	46	46	46	46
Riskiperusteinen tietosuoja	Korrelaatiokerroin	.492**	.479**	1.000	.616**	.692**
	P-arvo	.001	.001		.000	.000
	N	46	46	46	46	46
Tietosuojan ja tietoturvan välinen suhde	Korrelaatiokerroin	.751**	.660**	.616**	1.000	.808**
	P-arvo	.000	.000	.000		.000
	N	46	46	46	46	46
Sisäänrakennettu ja oletusarvoinen tietosuoja	Korrelaatiokerroin	.700**	.599	.692**	.808**	1.000
	P-arvo	.000	.000	.000	.000	
	N	46	46	46	46	46

** Korrelaatio on tilastollisesti merkitsevä 0.01 tasolla

6.1.3 Vastausten analysointi

Vastaajat ovat arvioineet väittämiä pitkälti samalla tavoin. Merkittävään osaan väittämistä on vastattu arvolla kolme – vastaajat eivät siis osanneet ottaa niihin kantaa. Myös hallintamallin osa-alueiden hajonnat ovat pieniä. Kun mediaani jää alle kolmen, on perusteltua tulkita, että rekisteröityjen oikeuksien toteutumisen kannalta tietosuojan kypsyystaso vastaa huonosti rekisterinpitäjälle tai tietojenkäsittelijälle asetettuja vaatimuksia.

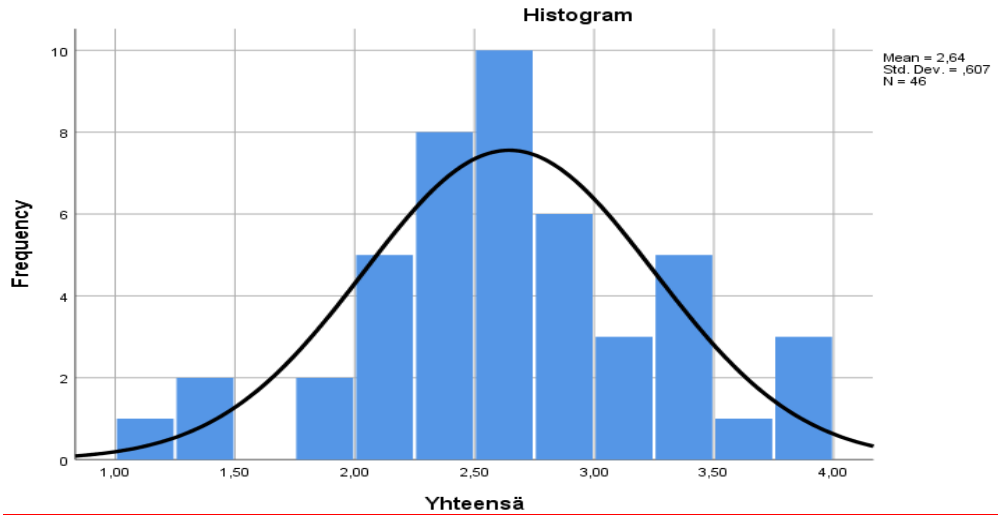


KUVIO 15. Yhteenveto vastausten keskiarvoista hallintamallin eri osa-alueilla

Vastausten keskiarvo hallintamallin osa-alueittain sijoittuu 2,48:n ja 2,97:n välille, mikä vastaa ilmauksia ”en ole samaa enkä eri mieltä” tai ”olen jokseenkin eri mieltä” (kuvio 15). Merkittävältä osin (koskee 49 %:a kaikista väittämistä) ei tietosuojan vaatimuksiin osata kohdeorganisaatiossa ottaa kantaa, vaikka tietosuoja-asetuksen mukaan potentiaalisten henkilötietojen käsittelyyn liittyvien riskienarviointien ja niiden hallintakeinojen tulee olla selvitettynä jo ennen pilvipalveluiden käyttöönottoa.

Koska väittämät on johdettu suoraan voimassa olevasta tietosuoja-asetuksesta sekä kansallisista tietosuojalaeista, on perusteltua olettaa, että vastaajat olisivat vähintäänkin jokseenkin samaa mieltä väittämien kanssa. Jotta tietosuojan vaatimustenmukaisuuden voidaan katsoa toteutuvan, tulee vastausten keskiarvojen olla yli neljä. Tulos osoittaa, ettei esitettyihin väittämiin osata pääsääntöisesti ottaa kantaa tai ollaan jokseenkin eri mieltä väittämän kanssa. Vastausten voidaan tulkita kertovan joko siitä, ettei kohdeorganisaation eri johtotasoilla ole tietoa, tunnetaanko organisaatiossa henkilötietojen käsittelyyn liittyviä toimintatapoja, tai siitä, että on olemassa todennäköinen riski tietojen käsittelyssä tapahtuvasta tietosuoja-asetuksen vastaisesta henkilötietojen käsittelystä.

Tarkasteltaessa vastausten keskihajontaa (kuvio 16) herää mielenkiinto jakauman ääripäitä kohtaan. Merkittävä osa vastauksista painottuu asteikon alkupäähän, ja hajonta on suurta. Vastaajat ovat siis merkittävästi joko eri mieltä tai täysin eri mieltä väittämien kanssa. Jotta sisäänrakennettu ja oletusarvoinen tietosuoja olisi vaatimustenmukaista, tulisi vastaajien olla vähintään samaa mieltä tai täysin samaa mieltä väittämän kanssa ja hajonnan tulisi olla pientä – koko käyrää pitäisi siis saada hilattua merkittävästi jakauman oikeaan reunaan päin ja hajontaa tulisi saada tiivistettyä.



KUVIO 16. Vastausten keskihajonta

Tarkasteltaessa aineistoa väittämätasolla kiinnittyy huomio siihen, että operatiivisen tietosuojan näkökulmasta vastaajat ovat keskimäärin yhtä mieltä kuin väittämä, että Valtorin ylimmällä johdolla on kokonaisvastuu vaatimuksen mukaisen tietosuojan toteuttamiseksi.

Vastaajat ovat jokseenkin eri mieltä siitä, että he ovat saaneet tarpeeksi informaatiota EU:n mallisopimuslausekkeiden hyödyntämisestä. Vastaajilla ei näytä olevan tarpeeksi informaatiota Privacy Shield -järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyyn eikä riittävästi informaatiota, jonka perusteella he kykenisivät arvioimaan, käsitelläänkö pilvipalveluissa erityisiä (arkaluonteisia) henkilötietoja vaatimusten mukaisesti. Voidaankin tulkita, ettei tietosuojan kypsyystaso riitä tiedon hyödyntämiseen arvioitaessa, siirtyvätkö pilvipalveluihin kerätyt henkilötiedot EU-alueen ulkopuolelle, sekä arvioitaessa tämän vaikutuksia rekisteröityjen oikeuksiin.

Vastaajat ovat jokseenkin eri mieltä siitä, että Valtorin asiakkaille on selvä, milloin he ovat rekisterinpitäjiä käytettäessä pilvipalveluita. Vastaajat ovat jokseenkin eri mieltä myös siitä, että tietoturvan ja -suojan vuosikelloa noudatetaan sovitulla tavalla.

Vastaajat eivät koe eri toimijoiden olevan selvillä rooleistaan, vastuistaan ja velvoitteistaan henkilötietojen käsittelyssä pilvipalveluissa, eivätkä Valtorille pilvipalveluja toimittavat organisaatiot aina tunnista omaa rooliaan henkilötietojen

käsittelyssä tai heidän käsityksensä ovat jossain määrin ristiriidassa tietosuoja-asetuksen kanssa.

Tarkasteltaessa tietosuojaan liittyvää riskinarviota on merkillepantavaa, että vastaajat ovat jokseenkin eri mieltä siitä, että Valtorissa tunnistetaan jäännösriskit ja että jäännösriskien arviointien tulokset ovat saatavilla. Suurimmat haasteet liittyvät jäännösriskien mitigointikeinojen jatkuvaan seurantaan sekä kyseisten toimenpiteiden vaikuttavuuden seuraamiseen, jota ei käytännössä toteuteta lainkaan.

Valtorin strateginen johto tunnistaa tietosuojavastuunsa, mutta organisaatiossa ei ole määritelty normatiivisesti reunaehtoja, joiden perusteella rekisterinpitäjät ja tietojenkäsittelijät toimivat. Tämä johtaa epäselvyyksiin eri toimijoiden tietosuojavastuista ja velvoitteista. Osana tietoturvavastuitaan tulee organisaation johdon varmistaa, että tietosuojavastaavan rooli on kaikkien tiedossa, erityisten henkilötietojen käsittelyn vaatimukset tunnetaan ja että tietosuojakoulutus on systemaattista.

Seuraavaksi tarkasteltiin, minkä väittämien osuvuutta ja paikkansapitävyyttä vastaajat olivat arvioineet merkitsevästi tai melkein merkitsevästi eri tavoin. Tarkasteltavana ovat kaikkien vastaajien arviot sekä johtoryhmien (lähijohto, keskijohto ja strateginen johto) arviot. Väittämät luetellaan taulukossa 4.

TAULUKKO 4. Väittämät, joita vastaajaryhmät (lähijohto, keskijohto ja strateginen johto) arvioivat merkitsevästi tai melkein merkitsevästi eri tavoin

Väittämä	**Merkitsevyys**
Saan riittävästi informaatiota, jotta voin arvioida, miten turvallista pilvipalveluissa tapahtuvan henkilötietojen käsittely on. Väittämässä viitataan henkilötietojen siirtoon eri maantieteellisten alueiden välillä.	p=0.038* Tilastollisesti melkein merkitsevä ero kaikkien vastaajien välillä.
Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluiden tapahtuvan henkilötietojen pseudonymisoinnin tarpeen.	p=0.036* Tilastollisesti melkein merkitsevä ero kaikkien vastaajien välillä. Keskijohdon ja strategisen johdon välillä on tilastollisesti melkein merkitsevä ero, p=0.043* Lähijohdon ja strategisen johdon välillä on tilastollisesti merkitsevä ero p=0.01**
Kykenen toimimaan pilvipalveluiden henkilötietojen käsittelyn poikkeamatilanteissa	p=0.044* Tilastollisesti melkein merkitsevä ero kaikkien vastaajien välillä. Keskijohdon ja strategisen johdon välillä on tilastollisesti melkein merkitsevä ero p= 0.017* Lähijohdon ja strategisen johdon väillä on tilastollisesti melkein merkitsevä ero p=0.019*
Tunnen Valtorin henkilötietojen luovutusten prosessin.	p=0.038* Tilastollisesti melkein merkitsevä ero kaikkien vastaajien välillä. Keskijohdon ja strategisen välillä on tilastollisesti melkein merkitsevä ero p=0.013*

Väittämä	Merkitsevyys
Saan tarpeeksi informaatiota tarkoituksenmukaisen henkilötiedonkäsittelyn määrittelemiseksi pilvipalveluissa	p=0.027* Tilastollisesti melkein merkitsevä ero Keskijohdon ja strategisen johdon välillä on tilastollisesti melkein merkitsevä ero p=0.019* Lähijohdon ja strategisen johdon välillä on tilastollisesti merkitsevä ero p=0.009**
Valtorissa tietosuojatyö on proaktiivista.	p=0.033* Tilastollisesti melkein merkitsevä ero kaikkien vastaajien välillä. Keskijohdon ja strategisen johdon välillä on tilastollisesti merkitsevä ero, p= 0.010** Lähijohdon ja strategisen johdon välillä on tilastollisesti melkein merkitsevä ero, p=0.018*
Saan tarpeeksi informaatiota tarkoituksenmukaisen henkilötiedonkäsittelyn määrittelemiseksi pilvipalveluissa.	p=0.027* Tilastollisesti melkein merkitsevä ero kaikkien vastaajien välillä. Keskijohdon ja strategisen johdon välillä on tilastollisesti melkein merkitsevä ero p= 0.019* Lähijohdon ja strategisen johdon välillä on tilastollisesti merkitsevä ero, p= 0.008**
Kykenen toimimaan pilvipalveluiden henkilötietojen käsittelyn poikkeamatilanteissa.	p=0.044* Tilastollisesti melkein merkitsevä ero kaikkien vastaajien välillä. Keskijohdon ja strategisen johdon välillä on tilastollisesti melkein merkitsevä ero p= 0.019* Lähijohdon ja strategisen johdon välillä on tilastollisesti melkein merkitsevä ero, p=0.017*

Vastaajat olivat samaa mieltä seuraavien väittämien kanssa:

- Valtorin ylimmällä johdolla on kokonaisvastuu vaatimustenmukaisen tietosuojan toteuttamisesta.
- Organisaatiossa on tarvittava informaatio päätöksentekoa varten tietosuojan viitekehyksestä.
- Organisaatiossa kyetään toimimaan pilvipalveluiden henkilötietojen käsittelyn poikkeamatilanteissa.
- Organisaatiossa on kyky henkilötietojen käsittelyn määrittelemiseksi pilvipalveluissa.

Ristiriitaa syntyy kuitenkin verrattaessa väittämiä muihin samaa aihepiiriä koskeviin väittämiin, joissa on tilastollisesti merkitseviä eroja vastaajien välillä.

Strategisella johtotasolla ollaan lähes samaa mieltä siitä, että organisaatiossa kyetään toimimaan pilvipalveluiden henkilötietojen käsittelyn poikkeamatilanteissa (ka. 4,6). Muut vastaajat olivat jokseenkin eri mieltä väittämän kanssa (ka. 2,0).

Tarkasteltaessa kaikkien vastaajien näkemyksiä väittämistä, joissa on tilastollisesti merkitseviä eroja, ristiriitaa oli havaittavissa väittämän

- Valtorin ylimmällä johdolla on kokonaisvastuu vaatimusten mukaisen tietosuojan toteuttamisesta. (ka. 4,6)

ja seuraavien väittämien saamien keskiarvojen välillä:

- Asiakkaille on selvä, milloin he ovat rekisterinpitäjiä käytettäessä pilvipalveluita. (Vastaajat ovat lähes eri mieltä tämän välittämän kanssa; ka 2,0.)
- Ennen pilvipalveluiden käyttöönottoa organisaatio hyödyntää näyttöön perustuvaa tietoa arvioitaessa, siirtyvätkö pilvipalveluihin kerätyt henkilötiedot EU-alueen ulkopuolelle. (ka 2,0)
- Organisaatiossa on tarpeeksi informaatiota EU:n mallisopimuslausekkeiden hyödyntämisestä. (ka 2.0)
- Organisaatiossa on tarpeeksi informaatiota Privacy Shield -järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyssä. (ka 2,0)
- Organisaatiosta saa riittävästi informaatiota pilvipalveluissa käsiteltävien erityisten (arkaluonteisten) henkilötietojen käsittelyn vaatimustenmukaisuuden arvioimiseksi. (ka 2,0)
- Tietosuojavastaavan toimenkuva on tuotu selkeästi esille Valtorissa. (ka 2,5)
- Valtorissa järjestetään riittävästi tietosuojakoulutusta. (ka 2,5)

Jotta Valtorin ylimmällä johdolla voisi olla kokonaisvastuu vaatimusten mukaisen tietosuojan toteuttamisesta, tulee toimijoiden roolien, vastuiden ja velvoitteiden olla selkeät. Organisaation johdon tulisi olla samaa mieltä EU:n mallisopimuslausekkeiden hyödyntämisestä, erityisten henkilötietojen käsittelyn vaatimuksista, tietosuojavastaavan roolista sekä systemaattisen koulutuksen tarpeesta.

6.1.4 Vastausten hajonta ja tuloksen merkitys tietosuojatyössä

Väittämäarviointien hajonta kertoo puutteista kohdeorganisaation tietosuojatyössä. Valtorin eri johtotasoilla työskentelevät toimijat tarkastelevat tietosuojaa heterogeenisesti. Eri johtotasoilla on yhteneväinen näkemys siitä, että tietosuojan kokonaisvastuu on organisaation johdolla. Kuitenkin strategisen johdon vastausten suuri hajonta tässä väittämässä vaikuttaakin merkitykselliseltä, sillä oletuksena on, että ylin johto olisi samaa mieltä väittämän kanssa ja että hajontakin olisi pieni. Puolet kaikista vastaajista ei muodostanut kantaansa väittämän merkityksellisyydestä. Tämä on tulkittavissa siten, ettei vastaajilla ole yhteneväistä näkemystä tietosuojavastuistaan.

Merkillepantavaa on, että suuri osa vastaajista ei pitänyt merkityksellisenä sitä, että organisaation johdolla tulee olla kokonaisvastuu henkilötietojen käsittelystä ja rekisteröityjen oikeuksien toteuttamisesta. Kaikista vastaajista 68 % sekä strategisista johtajista 85 % piti rekisteröidyn oikeuksien huomioimista päätöksentekoprosesseissa merkityksellisenä.

EU-tuomioistuin pitää henkilötietojen päätymistä EU-alueen ulkopuolelle rekisteröidyn oikeuksien kannalta merkittävänä riskinä. Tämä asia on olennaisen tärkeä jokaiselle henkilötietoja pilvipalveluissa käsittelevälle organisaatiolle. Rekisteröidyn oikeuksien suojaaminen oli keskeisin kriteeri Privacy Shield -järjestelyn kumoamiselle. Kumoamispäätöksellä on fundamentaalinen vaikutus tietosuojatyön strategiseen johtamiseen, ja siksi tuleekin kiinnittää huomiota siihen,

ettei 8 % Valtorin strategisen johdon edustajista pitänyt merkityksellisenä saada informaatiota Privacy Shield -järjestelyn kumoutumisen vaikutuksista. Lisäksi 31 % strategisesta johtotasosta, 12 % keskijohdosta sekä 15 % lähijohdosta ei pitänyt merkityksellisenä saada aiheesta näyttöön perustuvaa tietoa.

EU:n mallisopimuslausekkeiden hyödyntämisen merkitys Privacy Shield -järjestelyn kumoutumisen jälkeen näyttää jääneen kaikilla johtotasoilla epäselväksi. Strategisesta johtotasosta 54 % pitää merkityksettömänä EU:n mallisopimuslausekkeiden hyödyntämiseen liittyvän informaation saamista päätösten pohjaksi, vaikka ne ovat ainoita linjauksia, joilla kansallinen tietosuojaviranomainen on toistaiseksi ohjeistanut henkilötietojen käsittelyä pilvipalveluissa.

Ristiriitaa on havaittavissa tarkasteltaessa väittämiä, jotka liittyvät henkilötietojen siirtämiseen EU-alueen ulkopuolelle. Merkittävä osuus (41 %) vastaajista pitää merkityksellisenä, että he voivat hyödyntää näyttöön perustuvaa tietoa arvioidessaan henkilötietojen siirtoa EU-alueen ulkopuolelle. Kuitenkaan käytössä olevaa informaatiota, eli mallisopimuslausekkeiden hyödyntämiseen liittyvää informaatiota, ei juurikaan arvioida merkitykselliseksi. Lähijohdosta noin puolet (49 %) ei kommentoinut väittämän merkityksellisyyttä, vaikka asia koskee heitä erityisesti, sillä he toimivat operatiivisesti henkilötietojen käsittelijöinä.

Selitystä tälle on syytä hakea siitä, että ne asiantuntijat, joiden tehtävänä on operationalisoida oletusarvoinen ja sisäänrakennettu tietosuoja pilvipalveluissa, näyttävät jäävän paitsi tarvitsemastaan informaatiosta. Vastaajien koulutustaso, arvio omasta tietosuojaosaamisestaan sekä se, kuinka usein he käsittelevät tietosuojaan liittyviä kysymyksiä työssään, antavat ymmärtää, että EU:n tietosuoja-asetus sekä kansalliset tietosuojalait huomioitaisiin Valtorissa vaatimustenmukaisesti. Tutkimusaineisto ei kuitenkaan tue tätä käsitystä. Analyysi osoittaa, etteivät vastaajat ole sisäistäneet rekisteröidyn oikeuksia koskevia vaatimuksia.

Tietosuojatyön kokonaisvaltainen vaatimuksenmukaisuus vaihtelee tuotteistettujen palveluiden välillä, koska yksiköiden tietosuojan kypsyystasot ovat heterogeenisia ja toisistaan poikkeavia ja hajontakin on merkitsevää. Tietosuojan vaatimuksiin ei suurelta osin (koskee 49 % kaikista väittämistä) osata ottaa kantaa tai ne huomioidaan vasta pilvipalvelun käyttöönoton jälkeen, vaikka henkilötietojen käsittelyn riskinarvioinnin ja riskienhallintakeinojen tulee olla yksi käyttöönoton reunaehto.

Valtorin toimiessa rekisterinpitäjänä tai tietojenkäsittelijänä tarjoamissaan pilvipalveluissa, syntyy asymmetrisesti eri määrä vakavuudeltaan eritasoisia poikkeamia, koska tietosuoja ja tietoturva ovat heikosti vuorovaikutuksessa toistensa kanssa. Pahimmillaan vaatimukset ovat keskenään ristiriidassa ja vuorovaikutus eskaloituu kiistaksi.

Valtorin toimiessa rekisterinpitäjänä henkilötietojen käsittelylle asetettuja vaatimuksia ei aina ole yksiselitteisesti artikuloitu. Sama on todettavissa tarkasteltaessa kypsyyttä toteuttaa tietosuoja-asetuksen osoitusvelvoitetta, kun Valtori ja sen käyttämät toimittajat toimivat tietojenkäsittelijänä rekisterinpitäjän lukuun. Tämä näkyy konfliktina eri toimijoiden välisissä tietosuojarooleissa, -vastuissa sekä -velvoitteissa käytettäessä pilvipalveluita.

Proaktiivinen tietosuojatyö ja siihen liittyvä ennaltaehkäisevä työ ovat keskeisiä koko organisaatiossa. Vastaajista 68 % pitää proaktiivista tietosuojatyötä merkityksellisenä, ja sama trendi näkyy arvioitaessa ennaltaehkäisevän tietosuojatyön tärkeyttä. Strategisesta johdosta 92 %, keskijohdosta 73 % sekä lähijohdosta 51 % pitää ennaltaehkäisevää tietosuojatyötä merkityksellisenä.

Koska tietosuojatyö perustuu EU:n tietosuoja-asetuksen artiklan 24 mukaiseen henkilötietojen käsittelyyn liittyvien riskien arviointiin, kiinnittyy huomio siihen, että vastaajat ovat jokseenkin eri mieltä kuin väittämä, että Valtorissa saadaan riittävästi informaatiota tietosuojan jäännösriskien arvioinneista sekä jäännösriskien vaikutuksesta rekisteröityjen oikeuksiin ja vapauksiin.

Analysoitaessa vastauksia, jotka koskevat henkilötietojen käsittelyn ja säilyttämisen vaatimustenmukaisuutta pilvipalveluissa, törmätään ristiriitaan. Keskeinen henkilötietojen käsittelyn ja säilyttämisen arvioinnin väline on henkilötietovirtakaavio. Rönkön, Kinnusen, Kiviharjun ja Mäkisen (2016) mukaan tietovirtojen kuvaaminen auttaa ymmärtämään monimutkaisia henkilötietojen käsittelytoimia ja hallitsemaan tietosuojaa paremmin. Tietovirtakartan piirtäminen auttaa tietosuoja-asetuksen vaatimusten täyttymisen arvioinnissa ja riskien tunnistamisessa. Tietovirtakaavio on keskeinen väline henkilötietovirtojen inventoinnissa, minkä vuoksi sen kuvaaminen ja jatkuva ylläpitäminen on merkityksellistä tietosuojatyössä. (Rönkkö ym. 2016.)

Vastaajista 51 % piti merkityksellisenä tietoa siitä, onko tietojen säilytys vaatimustenmukaista, mutta 31 % vastaajista ei tunnistanut tietovirtakaaviota. Tärkeäksi havainnon tekee se, että ilman henkilötietovirtakaaviota ei tiedetä, missä henkilötiedot kulkevat. Kaikista vastaajista 60 % jätti arvioimatta, onko henkilötietojen käsittely kuvattu tietovirtakaaviona. Strategisesta johdosta 23 %, keskijohdosta 51 % sekä lähijohdosta 19 % pitää kyseistä väittämää merkityksellisenä päätöksentekoprosessissa.

6.2 Haastattelututkimus

Tutkimuksen validiteetin vahvistamiseksi toteutettiin triangulaatio, jossa määrällisen aineiston analyysin tuloksia täydennettiin teemahaastatteluilla. Tutkimuksen laadullisessa osassa aineistoa tarkastellaan tietosuojan viitekehyksistä.

Laadullinen tutkimus koostui kahdentyyppisistä haastatteluista: kuudesta yksilöhaastattelusta sekä yhdestä neljän hengen ryhmähaastattelusta. Haastateltavat olivat muualla kuin Valtorissa työskenteleviä asiantuntijoita. Heitä pyydettiin arvioimaan sekä ensimmäisen vaiheen tutkimustuloksia että oman organisaationsa tietosuojan kypsyystasoa.

Laadullisessa tutkimuksessa kysymyksenasettelu on avoin, toisin kun määrällisessä tutkimuksessa, jossa hypoteesien todentaminen perustuu aikaisempaan teoriaan tai kokemusperäiseen esiymmärrykseen (Eskola & Suoranta 1998; Metsämuuronen 2006). Siinä ei pyritä tilastollisiin yleistyksiin, ja ilmiön kuvaamiseksi voi riittää muutaman ihmisen haastattelu riippuen tutkittavasta ilmiöstä (Eskola & Suoranta 1998; Metsämuuronen 2006). Laadullisessa tutkimuksessa

riittävää aineiston määrää arvioidaan saturaation avulla. Aineisto katsotaan riittäväksi, kun uudet tapaukset eivät tuo tutkittavaan ilmiöön mitään uutta. (Eskola & Suoranta 1998, 62–68; Metsämuuronen 2006.) Metsämuurosen (2002, 177) mukaan laadullinen aineisto on kysymysten luonteen vuoksi rikkaampaa kuin määrällinen aineisto. Laadullisessa tutkimuksessa kysymykset pidetään avoimina ja haastateltavat voivat tuoda vastauksissaan subjektiivisia näkemyksiään esiin paremmin kuin valmiiksi strukturoiduissa kysymyksissä, joihin vastaaja vastaa tietyn asteikon mukaisesti.

Laadullisen tutkimusosion tarkoituksena on sekä syventää että vahvistaa tai kumota työn määrällisen osion tulosten analyysiä. Vastaajien erilaiset näkemykset auttavat tuomaan esille, millainen rooli tiedolla johtamisella on valtionhallinnossa, kun pilvipalveluissa toteutetaan oletusarvoista ja sisäänrakennettua tietosuojaa.

Laadullisessa tutkimuksessa tunnistetaan kaksi vaihetta, joista ensimmäinen on havaintojen pelkistäminen ja toinen on arvoituksen ratkaiseminen (Alasuutari, 2011, 39). Jotta tutkimusta voidaan tarkastella laajemmasta perspektiivistä ja yleisemmällä tasolla, on raakahavainnot pelkistettävä yhdistelemällä ne metahavainnoiksi (Alasuutari 2011, 184).

Haastatteluaineiston analyysin perusteella pyritään selvittämään arvoitus, ovatko määrällisen tutkimuksen tulokset yleistettävissä muuhunkin valtionhallintoon ja miksi ovat tai eivät ole. Tavoitteena on hahmottaa, löytyykö merkityksellisiä eroja tavoissa, joilla sisäänrakennettua ja oletusarvoista tietosuojatyötä toteutetaan valtionhallinnossa. Arvoituksen ratkaisemiseksi on selvitettävä, mistä erot syntyvät.

Koska aiheesta ei ole juurikaan julkaistu aiempaa tutkimusta kuvatussa laajuudessa, lähestyttiin ilmiötä tässä tutkimuksessa induktiivisen päättelyn kautta. Induktiivinen eli aineistolähtöinen analyysi sopii käytettäväksi silloin, kun aikaisempi tieto aiheesta on niukkaa tai hajanaista. Laadullinen aineistolähtöinen analyysi toteutetaan ilman ennakko-oletuksia tai määritelmiä, mikä tarkoittaa pelkistetyimmillään teorian rakentamista empiirisestä aineistosta käsin. Tällainen analyysi on tarkoituksenmukainen, kun tarvitaan perustietoa jonkin ilmiön olemuksesta tai siitä, mitä kyseinen ilmiö merkitsee. Menetelmä sopii tähän tutkimukseen, koska tarkoituksena on tuoda esiin tietosuoja-asiantuntijoiden subjektiivisia näkemyksiä tiedolla johtamisesta sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamisessa. Perusteluna teemahaastattelun valintaan voidaan pitää sen lupausta tiedon syventämisestä.

Haastattelujen avulla pyrittiin siis avaamaan sisäänrakennetun ja oletusarvoisen tietosuojan merkitystä sekä kuvaamaan tutkittavaa ilmiötä sen käsitteiden merkitysten kautta. Merkitys taas on tapa tunnistaa omia kokemuksia: merkitykset syntyvät siitä, millä tavoin yksilö arvioi omaa toimintaansa ja kokemaansa ja millä tavoin hän jäsentää sitä. (Morgan & Smircich 1980.)

Eri virastojen asiantuntijoiden tietosuojaan liittyvien käsitysten tutkiminen on merkityksellistä siksi, että käsitteellistäminen tuo esiin eri toimijoiden näkemyksiä ja tulkintoja tietosuojatyöstä. Käsitysten tarkasteleminen auttaa

ymmärtämään haastateltavien todellisuutta ja samalla myös ymmärtämään heidän toimintaansa tietosuojatyössä.

Kakkori ja Huttunen (2014) toteavat, että tutkimusprosessia voidaan kuljettaa eteenpäin hermeneuttiseen fenomenologiaan liittyvällä orientaatiolla tutkimusaineiston käsittelyssä. Käsitykset muodostuvat niistä merkityksistä, joita haastateltavat liittävät kokemuksiinsa tutkittavasta ilmiöstä, jolloin käsitykset kuvaavat tutkittavien todellisuutta. Tässä tutkimuksessa kuvattavana kohteena ovat ne merkitykset, joita sisäänrakennettu ja oletusarvoinen tietosuoja haastateltavien kuvaamana saa. Esitetty tapa lähestyä tutkittavaa ilmiötä on perusteltu, sillä käsitys usean samanaikaisen todellisuuden olemassaolosta ja todellisuuden subjektiivisuudesta johtaa tiettyihin oletuksiin myös tiedon luonteesta. Jos todellisuus ymmärretään moninaiseksi, myös tieto ja tietäminen rakentuvat subjektiivisesti. (Frey ym. 2000.)

Laadullisessa tutkimuksessa kysymykset tutkimuksen reliabiliteetista ja validiteetista on asetettava toisin kuin määrällisessä tutkimuksessa. Laadullisessa tutkimuksessa korostuvat analyysin systemaattisuuden ja tulkinnan luotettavuuden kriteerit. Tutkimuksen lukijalle osoitetaan, mistä aineisto koostuu, ja kuvataan aineiston osat, joiden varaan päähavainnot rakentuvat. Arvioitaessa tutkimuksen validiteettia mielenkiinto kohdistuu kerättyyn aineistoon ja niistä tehtävien tulkintojen johdonmukaisuuteen. (Ruusuvuori ym. 2011, 26–27; Heikkilä 2014.)

Laadullisella tutkimusotteella haluttiin selvittää, ymmärretäänkö sisäänrakennettu ja oletusarvoinen tietosuoja samankaltaisesti laajemmin valtionhallinnossa. Pyrkimyksenä oli myös ymmärtää, ovatko Valtorissa esille nostetut aspektit yleistettävissä laajemmin valtionhallinnossa.

6.2.1 Aineiston keruu ja käsittely

Teemahaastatteluun kutsuttiin vuosina 2021–2022 yhteensä kymmenen osallistujaa. Heistä kuusi oli satunnaisotannalla valittuja valtionhallinnossa työskenteleviä tietosuoja-asiantuntijoita, ja heitä haastateltiin **yksilöhaastatteluissa**. Lisäksi haastatteluun kutsuttiin yksi neljän hengen ryhmä yksityisestä yrityksestä, joka toimii ICT-palvelutalona, ja heitä haastateltiin **ryhmänä**. Ryhmähaastattelun osallistujat olivat teknisiä ICT- ja tietosuoja-asiantuntijoita, ja heidän haastattelemisensa tarkoituksena oli rikastaa käsitystä valtionhallinnon kypsyystasosta kolmannen osapuolen näkemyksellä teknisestä tietoturvan viitekehyksestä.

Haastattelut toteutettiin Teams-videoneuvotteluteknologian avulla, ja ne nauhoitettiin haastateltavien suostumuksella. Kukin haastattelu pyrittiin pitämään maksimissaan 60 minuutin mittaisena. Haastatteluiden alussa sovittiin, että haastateltavan yksityisyys varmistetaan anonymisoimalla yksilöitävät henkilötiedot. Haastatteluita jatkettiin, kunnes vastauksissa voitiin todentaa saturaatio.

Teemahaastattelut tehtiin lomakehaastattelun sekä avoimen ja semistrukturoidun haastattelun yhdistelmänä. Semistrukturoidussa teemahaastattelussa

haastateltaville esiteltiin ne 25 väittämää, joiden mediaani oli määrällisessä tutkimuksessa ollut ≥ 3,7 ja ≤ 2,5.

Lisäksi haastatteluissa esitettiin seuraavat avoimet kysymykset:

1. Mitkä tekijät ohjaavat organisaatiosi tietosuojatyötä?
2. Miten tietosuojaa toteutetaan organisaatiossasi? (Onko ohjauksessa ja toteutuksessa ristiriitoja?)
3. Millainen merkitys tiedolla johtamisella on tietosuojatyössä virastossasi?
4. Kuvaile organisaatiosi sisäänrakennettua ja oletusarvoista tietosuojatyötä.
5. Voiko julkisuudessa esitettyjä tietosuojapoikkeamia tapahtua virastossasi?

Aineisto litteroitiin, ja siitä määriteltiin analyysiyksiköt. Tässä tutkimuksessa analyysiyksikkönä on sana, lause tai teema. Analyysiyksikkö käsittää jossain tapauksessa useitakin lauseita eri merkityksineen tai myös lauseen osia (Hannila & Kyngäs 2008). Työssä ei tarkasteltu piilosisältöä, kuten esimerkiksi hiljaisuutta, huokauksia ja naurua.

Litteroinnin jälkeen aineisto pelkistettiin eli redusoitiin. Aineistosta louhittiin tutkimukselle relevantit kohdat, jotka esitetään taulukoissa 5 ja 6 pelkistettyinä havaintoina. Lähestymistapa helpottaa tutkimuksen kannalta epäolennaisen datan suodattamista pois, mikä tekee relevantin datan luokittelun, teemoittelun ja tyypittelyn laadukkaammaksi.

Pelkistetyt havainnot ryhmiteltiin niin, että identtiset ilmaukset muodostavat alaluokan. Tässä tutkimuksessa käytetään kolmea alaluokkaa: eksplisiittinen tieto, hiljainen tieto sekä kolmantena luokkana eksplisiittisen ja hiljaisen tiedon yhdistelmä. Työn fokuksena on tiedolla johtaminen tietosuojatyössä, ja siksi alaluokat muodostettiin tiedolla johtamisen teorian pohjalta.

Ryhmittelyvaiheessa alaluokat yhdisteltiin yläluokiksi ja niistä muodostettiin pääluokkia. Tässä tutkimuksessa yläluokat perustuvat Valtorin tietosuojan hallintamallin osa-alueisiin: hallinnollinen tietosuoja, operatiivinen tietosuoja, tietosuojan riskienhallinta, tietosuojan ja tietoturvan välinen vuorovaikutus sekä sisäänrakennettu ja oletusarvoinen tietosuoja.

Kaikki luokat nimettiin sisältöä kuvaavalla otsikolla. Niiden yhteiseksi otsikoksi tuli ”Havaintojen norminmukaisuus, yleistettävyys sekä ristiriidat” työn määrällisen osion kysymysten perusteella.

Pelkistäminen helpottaa ilmiön konstruoimista ja sääntöjen luomista ilmiölle. Kysymys siitä, miksi kohdeorganisaatiossa esiin tulleet näkökohdat joko ovat tai eivät ole yleistettävissä muuhun valtionhallintoon, ratkaistaan tulkitsemalla dataa hyödyntämällä Boolen algebraa, joka tarjoaa luotettavan menetelmän osoittaa väittämien yleistettävyys. Sitä hyödyntämällä maksimoidaan yleistysten tekeminen pienestä tutkittavasta aineistosta useiden eri vertailujen perusteella. Boolen algebra ottaa huomioon monien eri tekijöiden yhteisvaikutuksen, jonka perusteella kausaalisuus muodostetaan. Tämä auttaa generoimaan yleispäteviä ja kattavia tuloksia. Menetelmää pidetään kokonaisvaltaisena, ja sen käyttö yksinkertaistaa monimutkaisten kausaalisuhteiden käsittelyä. (Malinen & Pyykkö 2010, 48–51.)

Yksilö- eli asiantuntijahaastattelujen tarkoituksena oli selvittää valtionhallinnossa toimivien tietosuoja-asiantuntijoiden näkemyksiä tekijöistä, jotka ohjaavat tietosuojatyötä, sekä kartoittaa, miten tietosuojaa käytännössä toteutetaan. Kysymysten tavoitteena on lisätä tutkijan ymmärrystä siitä, voidaanko ensimmäiseksi tehdyn määrällisen tutkimuksen tulokset yleistää laajemmin valtionhallintoon, noudattaako valtionhallinnon tietosuojatyö normeja, esiintyykö tietosuojatyössä ristiriitoja sekä mitkä tekijät ohjaavat organisaatiossa tietosuojatyötä. Tämä kysymys on merkityksellinen, koska tiedolla johtamisen menetelmillä voidaan vastata sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamiseen.

Yhteenveto yksilöhaastattelujen haastattelukysymyksistä, havaintojen pelkistämisestä ja luokittelemisesta sekä havaintojen norminmukaisuudesta (täyttääkö asiantila tietosuojasta annetut normit), yleistettävyydestä ja mahdollisista ristiriitaisuuksista on taulukoissa 5 ja 6.

TAULUKKO 5. Havaintojen analysointi kysymykselle Mitkä tekijät ohjaavat organisaatiosi tietosuojatyötä?

Havaintojen pelkistäminen	**Alaluokka**	**Yläluokka**	**Normatiivisuus**	**Yleistettävyys**	**Ristiriitaisuus**
EU:n tietosuoja-asetus	Eksplisiittinen tieto	Hallinnollinen tietosuoja	Normatiivista	Voidaan yleistää	
Kansallinen tietosuojalainsäädäntö, Valittu strategia (’tietoturva politiikka’)	Eksplisiittinen tieto	Hallinnollinen tietosuoja	Normatiivista	Voidaan yleistää	
Toimijoiden välinen luottamus	Hiljainen tieto	Hallinnollinen tietosuoja	Ei normatiivista	Voidaan yleistää	
Rekisteröityjen perusoikeuksien suojaaminen	Eksplisiittinen tieto	Hallinnollinen tietosuoja	Normatiivista	Voidaan yleistää	
Resurssit	Hiljainen tieto	Operatiivinen tietosuoja	Ei normatiivista	Voidaan yleistää	
Tietoturvallisuuden tarpeet	Hiljainen tieto	Operatiivinen tietosuoja	Ei Normatiivista	ei voida yleistää	Ristiriitaa toiminnassa

TAULUKKO 6. Havaintojen analysointi kysymykselle Miten tietosuojaa toteutetaan organisaatiossasi?

Havaintojen pelkistäminen	**Alaluokka**	**Yläluokka**	**Normatiivisuus**	**Yleistettävyys**	**Ristiriitaisuus**
Tiedon jakamisen kulttuuri	Hiljainen tieto	Sisäänrakennettu ja oletusarvoinen tietosuoja	Ei normatiivista	Voidaan yleistää	
Maineenhallinta	Hiljainen ja eksplisiittinen tieto	Tietosuojan riskienhallinta	Ei normatiivista	Voidaan yleistää	
Riskiperusteisuus	Hiljainen ja eksplisiittinen tieto	Tietosuojan riskienhallinta	Normatiivista	Voidaan yleistää	
Kriteeristöjen mukaiset ulkopuolisen toteuttamat tietoturva-arvioinnit	Hiljainen ja eksplisiittinen tieto	Operatiivinen tietosuojatyö	Normatiivista	Voidaan yleistää	
Vaikutustenarvioinnit	Hiljainen ja eksplisiittinen tieto	Operatiivinen tietosuojatyö	Normatiivista	Voidaan yleistää	
Koulutus	Hiljainen ja eksplisiittinen tieto	Operatiivinen tietosuojatyö	Normatiivista	Voidaan yleistää	
Tietosuojavastaavan roolin esilletuominen	Eksplisiittinen tieto	Operatiivinen tietosuojatyö	Normatiivista	Voidaan yleistää	
Tietosuojan varmistamiseen liittyvä työ, ohjemateriaali	Eksplisiittinen tieto	Operatiivinen tietosuojatyö	Normatiivista	Voidaan yleistää	
Toimintakentän jatkuva muuttuminen	Hiljainen tieto	Operatiivinen tietosuojatyö	Normatiivista	Voidaan yleistää	
Tietosuojan huomioiminen hankinnoissa	Eksplisiittinen tieto	Hallinnollinen tietosuoja	Ei normatiivista	Voidaan yleistää	
Olemassa olevan tiedon jakaminen	Hiljainen tieto	Hallinnollinen tietosuoja	Normatiivista	Ei voida yleistää	Ristiriitaa toiminnassa
Sidosryhmäyhteistyö	Hiljainen tieto	Hallinnollinen tietosuoja	Normatiivista	Ei voida yleistää	Ristiriitaa toiminnassa
Tietoturva tukee vahvasti tietosuojaa ja sen merkitys korostuu	Hiljainen ja eksplisiittinen tieto	Tietosuojan ja -turvan vuorovaikutus	Normatiivista	Voidaan yleistää	

Havaintojen pelkistäminen	Alaluokka	Yläluokka	Normatiivisuus	Yleistettävyys	Ristiriitaisuus
Tavoitteiden asettelu yhdessä tietoturvan kanssa	Hiljainen ja eksplisiittinen tieto	Tietosuojan ja - turvan vuorovaikutus	Normatiivista	Voidaan yleistää	
Ratkaisut haetaan vuorovaikutuksen kautta	Hiljainen tieto	Tietosuojan ja - turvan vuorovaikutus	Normatiivista	Voidaan yleistää	
Ympäristö pyritään toteuttamaan vaatimusten mukaiseksi	Hiljainen ja eksplisiittinen tieto	Hallinnollinen tietosuoja	Ei normatiivista	Voidaan yleistää	
Haasteeksi koetaan siiloutuminen	Hiljainen tieto	Operatiivinen tietosuojatyö	Normatiivista	Voidaan yleistää	Ristiriitaa toiminnassa

6.2.2 Haastattelujen tulosten analysointi

Tässä työssä keskeinen kysymys on, täyttääkö tietosuojatyö sille asetut normit eli onko se *norminmukaista*. Asiaa tarkastellaan aiemmin esitetyn tietosuojan hallintamallin viitekehyksestä.

Normatiivisen etiikan teoriat pyrkivät tarjoamaan ratkaisuperusteita käytännön ongelmiin, ja keskeisiin teorian kysymyksiin, joita ovat mm. millainen toiminta on hyvää tai oikeaa ja mihin meidän pitää pyrkiä. Normatiivinen informaatio edustaa yhteiskunnassa vallitsevan, yleisesti hyväksytyn käsityksen mukaista informaatiota (Haasio 2015, 4).

Normatiivisen etiikan lähtökohta on arvioida ja perustella arvoja ja normeja sekä kuvata, miten erilaisissa tilanteissa tulisi toimia. (Rydenfelt 2014; Tuovinen 2015; Järvinen 2020.)

Selkeimmin muuhun valtionhallintoon yleistettäviä normien mukaisesta toiminnasta kertovia havaintoja nousi kaksi: pyrkimys EU:n tietosuoja-asetuksen ja kansallisen tietosuojalainsäädännön tinkimättömään noudattamiseen sekä rekisteröityjen perusoikeuksien turvaamiseen. Haastattelun analyysien perusteella vahvistui, että organisaatiot määrittelevät tietosuoja-asetuksen mukaisesti tietosuojatyön yhdeksi lähtökohdaksi riskiperusteisen tietosuojatyön, josta osoituksena on vaikutustenarviointien keskeinen rooli tietosuojatyössä. Tietosuojatyötä varmistetaan tuomalla esiin tietosuojavastaavan roolia sekä pyrkimällä vaatimukset täyttävään toimintaympäristöön. Puutteeksi näyttää kuitenkin nousevan se, seurataanko vaikutustenarviointien kautta tunnistettujen jäännösriskien poistamiseen määriteltyjen toimenpiteiden toteutumista, sekä toimenpiteiden vaikuttavuuden seuranta päivittämällä vaikutustenarvioinnit.

Haastateltavien mukaan sekä Valtorissa että yleisemmin virastoissa työtavoissa huomioidaan tietosuoja ja sitä arvioidaan katselmoinneilla ja puuttumalla poikkeamiin. Tietosuojan ja tietoturvan välinen vuorovaikutus näyttää toteutuvan, ja turvallisuuskatselmoinnit suoritetaan kriteeristöjen mukaisesti ulkopuolisen tekemillä tietoturva-arvioinneilla.

Vaatimustenmukaisuutta, jota seurataan vaikutusten arvioinneilla, tavoitellaan tietosuojan ja tietoturvan vuorovaikutuksen lisäksi koulutuksilla sekä erilaisilla ohjemateriaaleilla. Tietoturva tukee vahvasti tietosuojaa, ja sen merkitys korostuu. Organisaatioilla on myös omat poikkeamanhallintaprosessinsa.

Tiedolla johtaminen määritellään erittäin laveasti, ja se nähdään laajana strategisen johtamisen välineenä – sillä ei spesifisti johdeta tietosuojatyötä. Haasteeksi yleisesti mainitaan toimintakentän jatkuva muuttuminen. Edellä kuvatut havainnot ovat haastateltavien mielestä siis yleistettävissä laajemminkin valtionhallintoon.

Yleistettävissä oleviin, ei-norminmukaisesta toiminnasta kertoviin havaintoihin katsotaan kuuluvaksi havainnot, joissa vastaajat vaikuttavat puhuvan samasta asiasta, mutta syvempi tarkastelu osoittaa, että he tarkastelevat sitä eri perspektiivistä ja näin ollen myös tulkitsemisessa on näkemyseroja. Nämä havainnot voidaan yleistää, koska haastateltavat käyttivät niistä kuitenkin samaa käsitettä. Eri tavoin on tulkittu toimijoiden välistä luottamusta, sidosryhmäyhteistyötä, käytössä olevia tietosuojaresursseja, maineenhallintaa sekä sitä, miten tietosuojan huomioiminen hankinnoissa tuodaan esille.

Havaintojen perusteella voidaan todeta, että organisaatioiden ylin johto seuraa tietosuojatyötä aktiivisesti tiedolla johtamisen kautta. Tutkimus ei kuitenkaan tuottanut selkeää näyttöä siitä, että tietosuojatyötä ohjattaisiin tiedolla johtamisen avulla. Tiedolla johtaminen nähdään sen sijaan laajempana strategisen johtamisen välineenä. Tiedolla johtamisen käsite saa haastateltavien puheessa erittäin lavean tulkinnan.

Määrällisen kyselyn vastaajien ja haastateltavien käsitykset tiedon jakamisen kulttuurin kehittämistarpeista sekä tiedon siiloutumisesta poikkeavat toisistaan merkittävästi. Haastateltavat toivat esille, että toimintaympäristöt pyritään järjestämään tietosuojan vaatimusten mukaisesti ja että oletusarvoinen ja sisäänrakennettu tietosuoja on mukana suunnittelussa. Näissä havaintojen sisällöissä on merkittävää poikkeamaa, mikä johtaa tulkintaan, etteivät kyseiset asiat täytä normeja.

Tutkimusaineistosta nousevat esille määrällisen tutkimuksen vastaajien ja haastateltavien ristiriitaiset arviot tiedon jakamisen kulttuurista, tiedon siiloutumisesta sekä sidosryhmäyhteistyöstä. Aineiston perusteella voidaan tulkita, että vastaajat kokevat organisaatioiden johdon seuraavan aktiivisesti tietosuojatyötä tiedolla johtamisen kautta. Selkeää näyttöä normit täyttävästä tiedolla johtamisesta tietosuojatyössä ei kuitenkaan ole, mikä johtuu käsitteen väljästä tulkinnasta. Haastateltavat rinnastavat tiedolla johtamisen usein raportointiin. Tiedolla johtamista ei koeta tai tunnisteta tietosuojatyön strategiseksi johtamisen välineeksi.

Haastateltavat tunnistivat sisäänrakennetun ja oletusarvoisen tietosuojan olevan mukana Valtorin tietosuojatyön suunnittelussa sekä omassa tietosuojatyössään. Ristiriitaa syntyi kuitenkin siinä, että haastateltavat eivät määritelleet sisäänrakennettua ja oletusarvoista tietosuojaa yhtenäisesti eivätkä maininneet asiayhteydessä proaktiivisuutta, ennaltaehkäisyä tai läpinäkyvyyttä, jotka ovat oletusarvoisen ja sisäänrakennetun tietosuojan käsitteitä. Haastateltavat pitivät

riskiperusteista tietosuojatyötä ennemmin poikkeamienhallintaprosesseina kuin ennaltaehkäisevänä, heikkojen signaalien ja varhaisten varoitusten todennäköisyyksien arviointina.

Haastatteluissa ilmeni, etteivät Valtorin ja muiden toimijoiden tietosuojan poikkeamanhallintaprosessit ole yhdenmukaisia. Kun tarkastellaan eri toimijoiden rooleja, vastuita ja velvoitteita pilvipalveluiden käytössä, on haastattelujen perusteella tunnistettavissa luottamuspulaa toimittajien, Valtorin sekä asiakkaiden välillä. Tämä nousi esille keskusteltaessa pilvipalvelusopimusten sisällöistä, joissa tulevat vahvasti esille kulttuurisidonnaiset sekä lainsäädännölliset ristiriidat.

Ristiriitojen voidaan kiteyttää muodostuvan siitä, että haastateltavat kommentoivat havaintoja merkittävältä osin sen hiljaisen tiedon perusteella, joka heille on lyhyessä aikaikkunassa muodostunut omien kokemustensa sekä myös osittain organisaatiokulttuurien kautta. Syvällistä kokemusta ei yksinkertaisesti ole vielä päässyt muodostumaan tietosuoja-asetuksen voimaan astumisen jälkeen.

Toisistaan poikkeavista näkökulmista huolimatta haastateltavien kokemuksista nousi esiin tiettyjä teemoja, jotka toistuivat haastattelussa. Yhdeksi yhdistäväksi teemaksi nousi kysymys, **voiko julkisuudessa kuvattuja tietosuojapoikkeamia tapahtua haastateltavien virastoissa**. Alla katkelmia haastateltavien avoimista vastauksista:

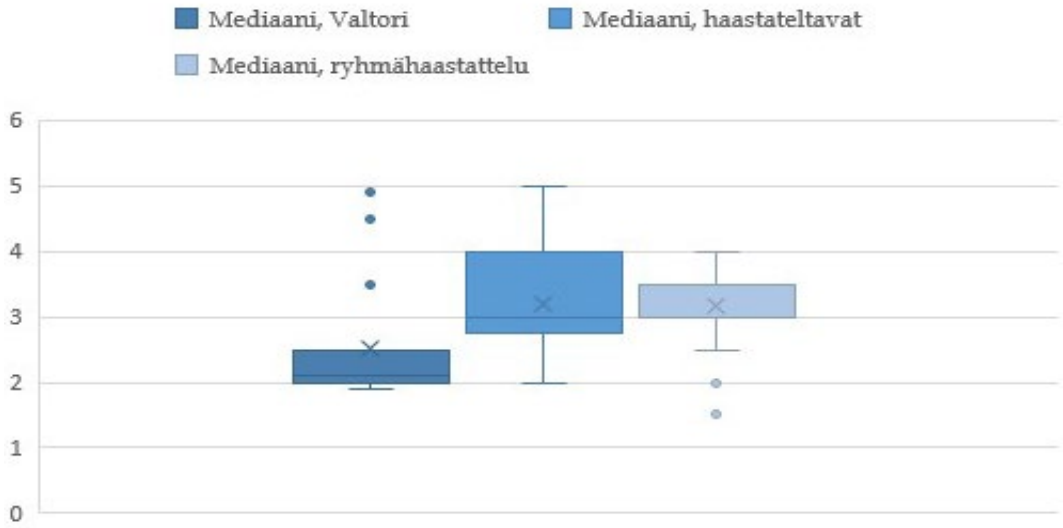
> ”On potentiaali, että jossain määrin voi toteutua.”
>
> ”Kaikkihan on mahdollista.”
>
> ”Tietosuojatyössä ei välttämättä ainakaan niin vahvasti näy siellä arjessa.”
>
> ”Tiedolla johtamisen näkökulmasta esimerkki, mikä voisi johtaa isoon poikkeamaan, on vaikka se, että me tunnistetaan, että tiettyinä kuukausina vuodesta meillä tapahtuu tietosuojaan liittyviä tietoturvaloukkauksia normaalia enemmän, jotka ovat luonteeltaan ja yksittäisinä tapahtumina vaikutukseltaan pieniä. Lähetetään väärää sähköpostia väärälle vastaanottajalle tai valtion virastossa lähetetään väärää aineistoa väärään paikkaan. Meidän pitäisi pystyä ennaltaehkäisemään nämä, siten että kun näitä tapahtuu, vaikka esimerkiksi kesäkuukausina, tunnistamme, että silloin siellä on harjoittelijoita tai tuuraajia. Tällöin pitää pystyä kohdentamaan koulutusta ja kontrolleja siihen porukkaan enemmän ja sitten se että OK. Tämä kertoo, että nämä poikkeamat ovat tämmöistä pientä väärään paikkaan lähettelyä, joka saattaa kuitenkin olla järkevää napata siitä kiinni. Mutta tämän tyyppiset asiat saattavat johtaa siihen, että jonain päivänä voi lähteä, vaikka tietyn viraston palkkaluettelo väärään sähköpostiosoitteeseen, joka ei olekaan valtionhallinnon sisällä. Tämä on erittäin konkreettinen esimerkki siitä, että jos tämä tieto (kesäkuukausina virheitä tapahtuu enemmän) kohtaa vastuullisen toimijan, voisi tieto johtaa siihen, että lisätään uuden tiedon perusteella perehdytystä. Perehdytyksen jälkeen sitten mitataan muutokset. Silloinhan tämä toimii juuri tiedolla johtamisen periaatteiden mukaisesti.”

”Mun olettama on se, että suomalaiset ei tiedä suinkaan, kuinka ohuella narulla tanssitaan tässä tietosuojan toteuttamisessa viranomaistoiminnassa. Mun mielestä nautitaan perusteetonta luottamusta tällä hetkellä, ja voisi olla hyvä, että johtokin saisi tietoa oikeasti, mitä ihmiset odottaa viranomaisilta. Kun odotuksia verrataan todellisuuteen, niin huomattaisiin, että ollaan melko kaukana siitä, mitä ehkä ajatellaan. Tämä tavallaan ei kestä kovin läpinäkyvää tarkastelua.”

6.2.3 Ryhmähaastattelu ja tulokset

Yksittäisten asiantuntijahaastattelujen lisäksi tehtiin yksi ryhmähaastattelu, johon osallistui neljä teknistä asiantuntijaa ICT-alan yrityksestä. Tällä pyrittiin syventämään tutkittavan ilmiön tarkastelua teknologisesta viitekehyksestä. Haastattelussa teknisiä asiantuntijoita pyydettiin arvioimaan kokonaisvaltaisen tietosuojan vaatimustenmukaisuutta, tietosuojan ja tietoturvan välistä vuorovaikutusta sekä sitä, täyttääkö tietosuojatyö sille asetetut normit, sekä kohdeorganisaatiossa että laajemmin valtionhallinnossa. Taustaväittäminä ja avoimina kysymyksinä käytettiin samoja kysymyksiä kuin tietosuoja-asiantuntijoiden haastatteluissakin (ks. alaluku 6.1). Haastattelutilanteessa haastateltavat keskustelivat jokaisesta käsiteltävästä väittämästä, kunnes he pääsivät konsensukseen. Täten muodostui ryhmän yhteinen kanta. Näkemykset eivät kuitenkaan edusta organisaation virallista kantaa.

Ryhmähaastattelussa vastaajat pääsääntöisesti tulkitsivat Valtorin kypsyystason olevan paremmalla tasolla kuin Valtorin henkilökunta itse arvioi sen olevan. Haastateltavat eivät osanneet ottaa kantaa 40 prosenttiin väittämistä. (Kuvio 17.)



KUVIO 17. ICT-palveluntarjoajien näkemys sekä Valtorin että muun valtionhallinnon tietosuojan vaatimustenmukaisuudesta

Seuraavassa on lueteltu tietosuojan vaatimuksenmukaisuutta kuvaavia väittämiä, jotka teknisten asiantuntijoiden mielestä toteutuvat Valtorissa, ja toisaalta väitteet, jotka toteutuvat siellä vain heikosti tai eivät lainkaan.

- Väittämä pitää paikkansa Valtorissa:
  - Ennen pilvipalveluiden käyttöönottoa Valtorissa hyödynnetään näyttöön perustuvaa tietoa arvioidessa, siirtyvätkö pilvipalveluihin kerätyt henkilötiedot EU-alueen ulkopuolelle.
  - Valtorin asiantuntijat saavat riittävästi informaatiota, jotta Valtorissa kyetään arvioimaan pilvipalveluissa käsiteltävien erityisten (arkaluonteiset) henkilötietojen käsittelyn vaatimustenmukaisuuden, pilvipalveluiden varmuuskopioiden ja lokien vaatimustenmukaisuuden arvioimiseksi sekä henkilötietojen minimikäsittelyn toteutumiseksi.
  - Tietosuojavastaavan toimenkuva on tuotu selkeästi esille Valtorissa.
  - Valtorissa järjestetään riittävästi tietosuojakoulutusta.
  - Käytettäessä pilvipalveluita osoitetaan Valtorissa näyttöön perustuen, että henkilötietojen minimikäsittelyn vaatimukset toteutuvat.
  - Valtorissa tiedetään, keneltä kysyä tietosuojaan liittyvää informaatiota.
  - Tietosuojatyössä tuotettu informaatio on Valtroissa päätöksentekoa varten merkityksellistä.
- Väittämä pitää paikkansa Valtorissa vain heikosti:
  - Valtorissa on tarpeeksi informaatiota Privacy Shield -järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyssä.
  - Valtorin ylimmällä johdolla on kokonaisvastuu vaatimusten mukaisen tietosuojan toteuttamiseksi.
  - Valtorin asiakkaille on selvää, milloin he ovat rekisterinpitäjiä käytettäessä pilvipalveluita.
  - Päätöksentekijät saavat Valtorissa riittävästi informaatiota tietosuojan jäännösriskien arviointia varten ennen pilvipalvelun käyttöönottoa sekä
  - Päätöksentekijät saavat Valtorissa riittävästi informaatiota pilvipalveluissa tapahtuvan henkilötietojen säilytyksen vaatimustenmukaisuuden todentamiseksi.
- Väittämä ei pidä paikkansa:
  - Valtorissa kyetään tunnistamaan potentiaalisia tietosuojapoikkeamia saadun informaation perusteella.

Tekniset asiantuntijat eivät kyenneet muodostamaan kantaa 40 prosentissa väittämistä, joiden perusteella Valtorin tietosuojan kypsyystasoa arvioidaan. Parhaiten he kykenivät muodostamaan näkemyksen seuraaviin väittämiin: asiakkaille on selvä, milloin he ovat rekisterinpitäjiä käytettäessä pilvipalveluita, organisaatiossa on käytössä riittävästi informaatiota tietosuojan jäännösriskien arviointia varten ennen pilvipalvelun käyttöönottoa sekä organisaatiossa on riittävästi informaatiota, jotta kyetään arvioimaan pilvipalveluissa tapahtuvan henkilötietojen säilytyksen vaatimustenmukaisuus.

Tekniset asiantuntijat ja Valtorin määrälliseen kyselyyn vastanneet olivat samaa mieltä siitä, ettei Valtorissa ole tarpeeksi informaatiota Privacy Shield -järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyyn, ettei Valtorin asiakkaille ole aina selvää, milloin he ovat rekisterinpitäjiä käytettäessä pilvipalveluita, ja etteivät päätöksentekijät saa Valtorissa riittävästi informaatiota tietosuojan jäännösriskien arviointia varten ennen pilvipalvelun käyttöönottoa sekä pilvipalveluissa tapahtuvan henkilötietojen säilytyksen vaatimustenmukaisuuden todentamiseksi.

Tekniset asiantuntijat ja Valtorin vastaajat olivat eri mieltä siitä, tunnistetaanko Valtorissa, että sen ylimmällä johdolla on kokonaisvastuu vaatimusten mukaisen tietosuojan toteuttamisesta sekä kyetäänkö Valtorissa ylipäätään tunnistamaan potentiaalisia tietosuojapoikkeamia saadun informaation perusteella.

Ryhmähaastattelussa teknisiä asiantuntijoita pyydettiin vertaamaan Valtorin tietosuojan kypsyystasoa muun valtionhallinnon organisaatioiden kypsyystasoon. Seuraavassa kuvataan ryhmähaastattelussa esiin tulleet merkittävät erot kohdeorganisaation ja muun valtionhallinnon tietosuojan kypsyystasossa:

- Valtorin kypsyystaso on korkeampi kuin valtionhallinnossa:
  - Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa käsiteltävien erityisten (arkaluonteiset) henkilötietojen käsittelyn vaatimustenmukaisuuden.
  - Valtorissa tunnistetaan jäännösriskit ennen pilvipalveluiden käyttöönottoa.
  - Tiedän keneltä kysyä tietosuojaan liittyvää informaatiota organisaatiossani.
  - Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluiden varmuuskopioiden ja lokien vaatimustenmukaisuuden.
- Valtorin kypsyystaso on matalampi kuin valtionhallinnossa:
  - Asiakkaille on selvä, milloin he ovat rekisterinpitäjiä käytettäessä pilvipalveluita.
  - Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa tapahtuvan henkilötietojen säilytyksen vaatimustenmukaisuuden.

Ryhmähaastattelussa ilmiön tarkastelun viitekehyksenä oli sekä tekninen tietoturva että globaalin liiketoiminnan mukanaan tuoma kansainvälinen lainsäädäntö. Haastattelussa kävi selväksi, että tekniset asiantuntijat kokevat EU:n tietosuoja-asetuksen olevan jossain määrin ristiriidassa muun kansainvälisen tietosuojalainsäädännön kanssa.

7 YHTEENVETO

Seuraavaksi vedetään yhteen kyselytutkimuksen ja haastattelututkimusten tuloksia, jotka esiteltiin luvussa 6. Alaluvussa 7.1 tuloksia esitellään laajemmin viiden teeman kautta ja alaluvussa 7.2 tiiviimmin Valtorin tietosuojatyön kannalta.

Lisäarvon tuottamiseksi suhteessa aiempiin tutkimuksiin tässä tutkimuksessa keskitytään tarkastelemaan ilmiötä tiedolla johtamisen näkökulmasta, mitä ei ole aiemmista tietosuojaan liittyvissä tutkimuksissa juurikaan tuotu esille. Tämän tutkimuksen analyysin tulokset vastaavat tutkimuskysymykseen Tiedolla johtaminen tarjoaa menetelmiä tietosuojatyön holistiseen tarkasteluun, joka konkretisoituu tässä tutkimuksessa sekä tietosuojan hallintamallin (kts. alaluku 2.2.2) että kehitetyn tietosuojatyön algoritmin kautta (kts. alaluku 8.2.1). Tutkimuksen analyysin tulokset vastaavat tutkimuskysymykseen ja havainnollistaa erilaisia toimintamalleja tietosuojan kypsyystason nostamiseksi sekä Valtorissa ja laajemminkin valtionhallinnossa. Tutkimuksen alkuperäinen kysymys koskee tietosuojatyössä tuotetun informaation saavutettavuutta sekä tiedolla johtamisen teorian hyödyntämistä oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamisessa. Viimeaikaisen kansainvälisen uutisoinnin perusteella kysymys on edelleen ajankohtainen ja aiheellinen. Analyysityö alkoi määrällisen aineiston tulkitsemisesta: mitä informaatiota eri päätöksentekijät tarvitsevat sekä mitä tietoa on saatavilla päätöksenteon tueksi sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamiseksi?

7.1 Aineiston tulosten esittely teemoittain

Tutkimuksen tulosten analysoinnissa nousi esille globaaleja tietosuojahaasteita, jotka ovat valtionhallinnossa Valtoria laajempia. Tosiasia on, että valtionhallinnon päätöksentekijöille on tarjolla tietosuojaan liittyvää informaatiota, jota he voivat hyödyntää toteuttaessaan pilvipalveluja rekisteröityjen oikeuksien sekä oletusarvoisen ja sisäänrakennetun tietosuojan mukaisesti. Vastaus tutkimuskysymykseen on silti kiteytetysti seuraava: kohdeorganisaation eri johtotasojen

tietosuojaosaamisen kypsyystaso ei kaikilta osin vastaa tietosuoja-asetuksen vaatimuksia, eikä eri johtotasojen käsitys tietosuojasta ole samansuuntainen.

Aineiston perusteella ei voida vahvistaa työn hypoteesia eli sitä, että kohdeorganisaation eri johtotehtävissä toimivat asiantuntijat pystyisivät muodostamaan saamansa informaation perusteella ammatillisessa roolissaan tarvitsemaansa tietoa vaatimustenmukaista tietosuojatyötä varten.

Tarkasteltaessa vastausten jakaumia tietosuojan hallintamallin osa-alueittain nähtiin, että merkittävään osaan niihin kuuluvista väittämistä on vastattu arvolla 3, joka käytetyllä asteikolla merkitsee, etteivät vastaajat osanneet ottaa väittämään kantaa. Osa-alueiden sisäisten hajontojen pienuus vahvistaa käsitystä siitä, että vastaajat ovat arvioineet väittämät samansuuntaisesti. Jos mediaani on alle 3, on perusteltua tulkita, että rekisteröityjen oikeuksien toteutumisen näkökulmasta Valtorin tietosuojan kypsyystaso vastaa huonosti rekisterinpitäjälle tai tietojenkäsittelijälle asetettuja vaatimuksia. Erisuuntaiset vastaukset korostavat vastaajien eriäviä käsityksiä toimijoiden tietosuojaan liittyvistä rooleista, vastuista ja velvoitteista.

Seuraavaksi tutkimusten tuloksia vedetään yhteen viiden teeman – tietojen siirtämisen, tietosuojalainsäädännön tuntemisen, informaation ja tiedon käsittelemisen, tiedolla johtamisen sekä yleisen tietosuojakompetenssin – kautta.

7.1.1 Tietojen siirtäminen EU:n ja ETA:n ulkopuolelle

Tutkimuksen perusteella epäselvin asiakokonaisuus on rekisteröityjen oikeuksien toteutuminen tietojen siirtämisessä. Kun tietoja siirretään EU- ja ETA-maista kolmansiin maihin, entistä kauemmaksi rekisterinpitäjästä, on ilmeinen vaara, etteivät tietosuojavaatimukset toteudu. Myöskään tietojenkäsittelyn lainmukaisuutta eikä käsittelyn läpinäkyvyyttä voida varmistaa, koska EU-alueen ulkopuolella noudatetaan EU:n tietosuoja-asetuksesta poikkeavaa lainsäädäntöä.

Määrällisen aineiston perusteella tehdyn tulkinnan perusteella haastateltavien keskuudessa vallitsi käsitys, että yhdysvaltalaiset palveluntarjoajat noudattavat ensisijaisesti Yhdysvaltojen lainsäädäntöä (mm. Cybersecurity Act, Kalifornian kuluttajien yksityisyyttä koskeva laki CCPA, Cloud Act, USA Patriot Act, HIPAA, FISA), joka on tietosuoja-asetukseen nähden osin ristiriitainen. Haastateltavat olivat yksimielisiä siitä, että tämä potentiaalinen ristiriita on ajankohtainen haaste useassa valtion organisaatiossa ja itse asiassa koko EU:n alueella. Riskin juurisyyksi tunnistetaan se, että ne pilvipalveluiden toimittajat, jotka tuottavat palveluita valtionhallintoon, ovat yhdysvaltalaisia ja noudattavat omaa lainsäädäntöään, joka merkittäviltä osin poikkeaa EU:n tietosuoja-asetuksesta.

EU-tuomioistuin kumosi Privacy Shield -järjestelyn vuonna 2020, ja Euroopan tietosuojaneuvosto julkaisi lisäohjeistusta, joiden mukaan mallilausekkeet (SCC) ovat edelleen pätevä suojamekanismi, kun tietoja siirretään EU- ja ETA-alueiden ulkopuolelle, mutta Yhdysvaltojen kohdalla tarvitaan myös lisäsuojakeinoja (supplementary measures). Soveltuvien lisäkeinojen pohtiminen ja mallilausekkeiden riittävyyden arviointi ovat sekä rekisterinpitäjän että tietojenkäsittelijän velvollisuus. Tietojen pääkäsittelijän, eli tietojenkäsittelijän, joka käsittelee tietoja rekisterinpitäjän lukuun, vastuulla on varmistaa, että tietojen

alikäsittelijät, Valtorin näkökulmasta toimittajat, täyttävät tietojenkäsittelylle asetetut vaatimukset, joihin keskeisesti liittyvät henkilötietojen maantieteellisen sijainnin määrittely ja sen varmentaminen, etteivät kyseiset tiedot siirry muualle. Euroopan komissio hyväksyi 10.7.2023 EU:n ja Yhdysvaltojen tietosuojan riittävyyttä koskevan päätöksen (”the EU-U.S. Data Privacy Framework”). Päätöksessä todetaan, että Yhdysvallat takaa EU:sta yhdysvaltalaisille yrityksille siirrettäville henkilötiedoille riittävän suojan tason, joka on verrattavissa Euroopan unionin suojaan (European Commission 2023a). Tämän tutkimuksen julkaisuhetkellä ei ole vielä julkaistu näyttöön perustuvaa tutkimustietoa päätöksen vaikutuksista rekisteröidyn oikeuksille tai vapauksille.

Puhuttaessa tiedonsiirroista kolmansiin maihin nousi haastattelututkimuksessa esille Transfer Impact Assessment (TIA) -prosessi, jossa arvioidaan henkilötietojen siirron vaikutuksia tietosuojan kannalta tunnistamalla mahdolliset riskit ja vaikutukset, joita henkilötietojen siirto voi aiheuttaa tietojen siirron aikana. Tavoitteena on tunnistaa mahdolliset riskit, kuten tietojen luvaton käyttö tai paljastuminen ja ryhtyä tarvittaviin toimenpiteisiin riskienhallinnan varmistamiseksi. TIA:n toteuttaminen vaatii, että organisaatioissa tulee olla käytettävissä osaamista eri maiden toisistaan merkittävästikin poikkeavan tietosuojalainsäädännön tulkitsemiseen.

Haastatteluissa tuli ilmi, että useampi virasto tunnustaa olevansa liian pieni toimija neuvottelemaan pilvipalveluiden sopimusehdoista toimittajien kanssa. Näyttää kuitenkin siltä, että globaalit pilvipalveluiden toimittajat neuvottelevat henkilötietojen käsittelyyn liittyvistä ehdoista mieluummin erikseen jokaisen jäsenmaan sisällä eri toimijoiden kanssa kuin EU-tasolla. Valitun strategian taustalla saattaa yksinkertaisesti olla globaalien toimijoiden markkina-asema, joka on johtanut ns. vendor lock-in-tilanteeseen, jossa asiakkaan on vaikea vaihtaa palvelun toimittajaa.

Sopimusehdoista neuvottelemisen vaikeuden juurisyy näyttää olevan se tosiasia, että Yhdysvalloissa kynnys henkilötietojen luovuttamiseen kolmansille osapuolille on matalampi kuin EU-alueella. EU:n tietosuoja-asetuksen kannalta katsottuna rekisteröidyn oikeudet ovat tällöin todennäköisesti uhattuna. Kysymys näyttääkin muodostuvan taloudellisen näkökulman ja yksityisyyden suojan väliseksi debatiksi. Yhteisenä nimittäjänä voidaan pitää eri virastojen kollektiivista huolta siitä, kykenevätkö kansainväliset pilvipalveluiden tarjoajat osoittamaan, että palvelu täyttää EU:n tietosuoja-asetuksen vaatimukset.

Arvioitaessa pilvipalveluiden hankintavaiheen riskejä nousi sekä määrällisestä että laadullisesta aineistosta esille, että pilvipalvelut mahdollistavat henkilötietojen virtaamisen EU-alueen ulkopuolelle, mikä on EU:n tietosuoja-asetuksen näkökulmasta jo toteutunut juridinen riski.

7.1.2 Tietosuojalainsäädännön tunteminen

Vastaajat eivät osanneet ottaa kantaa kaikkiin tietosuojalainsäädäntöä koskeviin väittämiin, esimerkiksi siihen, kykenevätkö he ennaltaehkäisemään tietosuojapoikkeamia saamansa informaation perusteella tai voidaanko Valtorissa osoittaa näyttöön perustuen, että henkilötietojen minimikäsittelyn vaatimukset

toteutuvat. Vastaajat eivät osanneet ottaa kantaa myöskään siihen, käsitelläänkö Valtorin käyttämissä pilvipalveluissa henkilötietoja käyttötarkoitussidonnaisesti, onko tietosuojatyö proaktiivista tai tunnistetaanko tietosuojaan liittyvät riskit ennaltaehkäisevästi.

Vastaajat eivät osanneet ottaa kantaa myöskään siihen, huomioidaanko Valtorin käyttämien pilvipalveluiden henkilötietojen käsittelyssä rekisteröidyn oikeudet, onko henkilötietojen käsittely Valtorin tarjoamissa pilvipalveluissa läpinäkyvää ja avointa, huolehditaanko Valtorin henkilötietojenkäsittelyssä tietojen elinkaaresta sekä kerätäänkö ja käsitelläänkö Valtorissa vain välttämättömiä henkilötietoja.

Uuden tietosuoja-asetuksen tulkinta on kaiken kaikkiaan monisäikeistä ja jossain määrin epäselvää niin Valtorin henkilökunnalle kuin ulkopuolisille haastateltavillekin. Sitä koskeva informaatio saattaa näyttää vastaajista kryptiseltä datamassalta, ja datamassaa kuvattiin pikemminkin lisätyötä aiheuttavaksi rasitteeksi kuin päätöksentekoa helpottavaksi informaatioksi. Kun informaatiosta jalostettua uutta tietoa ei juurruteta käytännön prosesseihin, on olemassa ilmeinen riski, ettei rekisteröidyn oikeuksia huomioida vaaditulla tasolla arkityössä.

Vastausten perusteella vastaajilla on kiinnostusta EU:n tietosuoja-asetusta kohtaan, mutta käytännössä asetukseen reagoidaan monin eri tavoin, mikä aiheuttaa varianssia siihen, miten hyvin tietosuojatyö täyttää sille asetetut normit. Ääripään kommenteissa mainitaan tietosuojan ja teknisen tietoturvan välillä esiintyvät konfliktit, ja lainsäädännön tulkinnan katsotaan jopa estävän tehokkaan teknisen tietoturvan toteuttamisen.

Eri toimijoiden, rekisterinpitäjistä pilvipalveluiden toimittajiin, tulee olla samaa mieltä myös käytettävistä tietoturvastandardeista ja -ohjeista. Muussa tapauksessa makrotasolla potentiaalisiksi riskeiksi nousevat tiedon elinkaareen, saavutettavuuteen, käytettävyyteen, tiedon minimikäsittelyyn ja käyttösidonnaisuuteen liittyvät riskit, resilienssiin ja käytettävyyteen liittyvät riskit sekä toimittajariippuvuuteen liittyvät riskit. Rekisterinpitäjän velvollisuutena on määritellä standardit ja ohjeet, joilla edellä mainittujen lakien vaatimukset saadaan täytettyä. Ne jäävät toteutumatta niin pitkäksi aikaa, kun ei ole yksimielisyyttä rekisterinpitäjyydestä.

Tutkimus osoittaa, ettei tietosuojan ja tietoturvan välinen vuorovaikutus ole Valtorissa kitkatonta, päinvastoin ääritapauksessa saatetaan jopa ajatella, että tietosuoja haittaa tietoturvan toteutumista. Haastattelun analyysi vahvistaa, että tämä ilmiö on tunnistettavissa laajemminkin valtionhallinnossa: sekä Valtorin ja virastojen välillä, että myös eri virastojen sisällä. Huomio on merkityksellinen, sillä merkittävä osa tietosuojavaatimuksista toteutetaan hallinnollisilla, fyysisillä tai teknisillä tietoturvakontrolleilla. Asetelma tulee tunnistaa heikoksi signaaliksi epäsuotuisasta kehityksestä, joka muodostaa toiminnallisen konfliktin. Tilanne on purettavissa lisäämällä tietosuojatyön läpinäkyvyyttä sekä tiedon jakamisen kulttuuria.

Edellä kuvatut tiedot liittyvät aiemmin esitettyyn huomioon siitä, että EU:n tietosuoja-asetusta ja sitä tarkentavaa ja täydentävää kansallista lainsäädäntöä tulkitaan heterogeenisesti. Ristiriitaisia toimintatapoja syntyy, jos toimijat ovat

eri mieltä henkilötietojen käsittelyn rooleista, vastuista sekä velvoitteista. Niitä ei ole kuvattu normatiivisesti esimerkiksi toimittajien ja asiakkaiden välisissä tietojenkäsittelysopimuksissa, jolloin sopimusteksti ei vastaa todellisuutta. Tämä johtaa siihen, että pilvipalveluiden toimittajien käyttöehtosopimuksia voidaan tulkita eri tavoin kuin tietosuoja-asetusta.

Haastattelut osoittavat, että tuloksia voidaan yleistää laajemmin valtionhallintoon: eri toimijat näyttävät tulkitsevan EU:n tietosuoja-asetusta eri näkökulmista sen mukaan, toimivatko he esimerkiksi taloushallinnossa, henkilöstöhallinnossa, asiakasrajapinnassa vai tuotannossa, ikään kuin katsoisivat samaa järveä eri rannoilta. Lisäksi globaaleilla pilvipalvelutoimittajilla on rekisteröidyn oikeuksista omat näkemyksensä, jotka lähtökohtaisesti perustuvat muuhun lainsäädäntöön.

Tietosuoja tunnistetaan sekä Valtorissa että laajemmin valtionhallinnossa periaatetasolla merkitykselliseksi. Tietosuoja-asetus näyttää olevan virastoille käsitteenä tuttu, mutta se mielletään kuitenkin vaikeaksi juurruttaa osaksi toimintaa. Viraston koolla ja tietosuojan kypsyystasolla näyttää olevan tässä korrelaatio. Suurimmilla virastoilla on paremmat mahdollisuudet resursoida tietosuojaan, mikä näkyy suoraan tietosuojan kypsyystasossa. Tämä ei kuitenkaan suoraan heijastu siihen, että eri virastojen välillä vallitsisi yksimielisyys toimijoiden rooleista, vastuista ja velvoitteista.

Kiinnostus asetusta kohtaan vaikuttaa olevan varsin abstraktia, eikä sen vaatimusten implementoinnille näy olevan yksiselitteisiä ratkaisuja. Harvat kyselyyn osallistuneet pitävät asetuksen mukanaan tuomia muutoksia mahdollisuutena. Kyselyn vastaajat kuitenkin tietävät, keneltä kysyä tietosuojaan liittyvää informaatiota Valtorissa.

7.1.3 Informaatio, tieto ja tiedon siiloutuminen

Vastaajat olivat jokseenkin samaa mieltä siitä, että tietosuojatyötä koskeva informaatio on heidän työssään päätöksentekoa varten merkityksellistä. Kohdeorganisaation kyky hyödyntää tietosuojatyötä koskevaa uutta tietoa näyttää kerätyn aineiston valossa kuitenkin heikolta.

Tietosuoja-asiantuntijat eivät tutkimusaineiston mukaan välitä tietosuojatyössä muodostunutta informaatiota eri asiantuntijoille niin, että se tukisi päätöksentekoa vaikuttavasti, eivätkä Valtorin eri johtotasoilla toimivat henkilöt tunnista, mikä tietosuojaan liittyvä informaatio on heidän päätöksentekoprosessiensa kannalta merkityksellistä. Voidaan myös kysyä, onko toimijoilla kypsyyttä hyödyntää käytössään oleva tieto ja onko informaatio juuri sellaista, jota kyseinen toimija tarvitsee normit täyttävään tietosuojatyöhön. Yli puolet kohdeorganisaation vastaajista piti tietosuojaosaamistaan joko hyvänä tai erinomaisena, mutta heidän käsityksensä oli ristiriidassa muun aineiston kanssa, joka ei vahvista heidän näkemystään. Tutkimuksessa ”en osaa sanoa” -vastausten määrä oli tässä huomattavan suuri. Ryhmähaastattelussa haastateltavat arvioivat Valtorin tietosuojan kypsyystason paremmaksi kuin Valtori itse, mutta he pitivät pääsääntöisesti oman organisaationsa kypsyystasoa korkeampana kuin Valtorin. Merkittävin osin väittämiin ei osattu kuitenkaan ottaa kantaa.

Tämän tutkimuksen johtopäätös on, että vielä ei olla vaaditulla kypsyystasolla eivätkä toimijat saa käyttöönsä juuri heidän tarpeitaan vastaavaa, datasta ja heikoista signaaleista jalostettua informaatiota päätöksenteon tueksi. Käytännössä tämä johtaa epävarmuuteen vastuun kantamisessa eikä tue proaktiivista tietosuojatyötä.

Analyysien tulosten pohjalta on siis perusteltua kysyä, kykenevätkö asiantuntijat Valtorissa ja laajemmin valtionhallinnossa muodostamaan saamastaan informaatiosta sellaista tietoa, jota he voivat käyttää päätöksenteon pohjana. Tähän näyttävät vaikuttavan seuraavat keskeiset tekijät: kykenevätkö asiantuntijat jäsentämään käytössään olevaa informaatiota päätöksentekoa varten relevantiksi tiedoksi, onko tietosuoja-asiantuntijoilla tarpeeksi tietosuojaosaamista ja viestintäosaamista, jotta he kykenevät artikuloimaan ja jäsentämään uutta informaatiota selkeäksi ja ymmärrettäväksi niin, että tietojenkäsittely olisi rekisteröidyn oikeuksien kannalta vaatimustenmukaista, sekä onko saatavilla oleva informaatio relevanttia ja validia? Näiden kysymysten jälkeen voidaan arvioida, saavatko asiantuntijat juuri heille päätöksentekoa varten merkityksellistä informaatiota. Koska tieto muodostuu saatavilla olevasta informaatiosta, merkittävään asemaan oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamisessa nousevat tiedon jakaminen ja hyödyntäminen sekä SECI-mallin ymmärtäminen.

Haastatteluissa todettiin, että EU:n tietosuoja-asetus ja sitä täydentävä kansallinen lainsäädäntö ovat yleisesti saatavilla ja niitä tulee noudattaa. Tämän pohjalta on perusteltua olettaa, että päätöksentekijöillä olisi käytettävissään tarvittava tietosuojaan liittyvä informaatio oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamiseksi. Haastattelut kuitenkin indikoivat, etteivät tutkimuksen kohdeorganisaation, Valtorin, eri johtotasoilla toimivat henkilöt saa tarvittavaa informaatiota sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamiseksi tai että he eivät pidä informaation sisältöä relevanttina. Se, mikä tietosuojaan liittyvä informaatio on heidän työnsä kannalta merkityksellistä, on jäänyt haastatteluun osallistuneille vastaajille epäselväksi.

Aineistoista haettiin tietoa siitä, käytetäänkö tiedolla johtamisen osana myös tietosuojatiedon jakamista. Tutkimuksen pohjalta voidaan sanoa, että Valtorissa on havaittavissa siiloutumista eli tiedonkulun esteitä. Siiloutumista voidaan haastattelujen perusteella havaita myös laajemmin valtionhallinnossa. Vastakohtana toimintaa heikentävälle siiloutumiselle tiedon jakamisen kulttuuri johtaisi organisaation kokonaisvaltaiseen kehittymiseen. Avoimuus ja toiminnan läpinäkyvyys, joihin tiedon jakaminen tähtää, tukisi ja edistäisi yhteisten tavoitteiden saavuttamista.

7.1.4 Tarkastelua tiedolla johtamisen näkökulmasta

Tietosuojatyössä tiedolla johtamisen teorian hyödyntämisen haasteena näyttää olevan se, että tiedolla johtamisen teoriaa tulkitaan Valtorissa varsin laveasti tai sitä ei tunneta lainkaan. Se mielletään Valtorissa, ja laajemminkin valtionhallinnossa, ennemminkin erilaisten geneeristen raportointityökalujen käyttämiseksi kuin strukturoiduksi prosessiksi, jossa tieto välittyy vuorovaikutuksessa ulkoiseen muotoon ja josta opitaan uutta.

Kausaliteetin tulkitseminen osoittautui tässä tutkimuksessa merkitykselliseksi. Ennen kuin voidaan arvioida, mikä tietosuojaan liittyvä informaatio on päätöksentekoprosessissa merkityksellistä, on selvitettävä, miksi valtionhallinnossa tietosuojan kypsyystaso ei vaikuta tutkimuksen tulosten perusteella olevan vaatimustenmukaista. Tässä tutkimuksessa ehdollisesta kausaalikäsityksestä voidaan esittää seuraava esimerkki:

Syy: Organisaation tietosuojan kypsyystaso (maturiteetti) ei riitä asiantuntijoiden tuottaman tietosuojainformaation hyödyntämiseen. Tiedolla johtamisen teoriaa ei hyödynnetä spesifisti tietosuojatyössä.

Seuraus: Sisäänrakennettu ja oletusarvoinen tietosuoja ei toteudu.

Missä olosuhteissa kausaalisuhde pätee: Kun organisaation tietosuojan kypsyys ei ole vaaditulla tasolla.

Ennen kuin voidaan edes harkita tiedolla johtamisen teorian hyödyntämistä tietosuojatyössä, on organisaatioiden tietosuojan kypsyyttä kyettävä nostamaan ja tietosuojatyön norminmukaisuutta lisäämään harmonisoimalla toimintaa. Tiedolla johtamisen teoriaa ei voida hyödyntää interventioissa, ennen kuin tietosuojatyön voidaan osoittaa olevan vaatimustenmukaista.

7.1.5 Tietosuojan edellyttämä vahva kompetenssi

Tutkimuksen tulokset antavat ymmärtää, ettei päätöksentekijöillä ole vahvaa kompetenssia varmistaa oletusarvoisen ja sisäänrakennetun tietosuojan toteutumista pilvipalveluissa käytössään olevan informaation perusteella. Tämä antaa selkeitä viitteitä, ettei Valtorin tietosuojatyössä riittävästi toteudu oletusarvoisen ja sisäänrakennetun tietosuojan periaatteet: proaktiivisuus, ennaltaehkäisy, läpinäkyvyys ja riskilähtöisyys. Yksittäiset haastateltavat eri virastoista tosin ilmaisivat toteuttavansa periaatteita intuitiivisesti. He eivät kuitenkaan osanneet nimetä niitä.

Samat neljä periaatetta ovat käytössä kriisinhallinnan teorioissa. Koska rekisteröityjen oikeuksien ja vapauksien rikkominen voi pahimmillaan todella aiheuttaa kriisin, ongelmia on johdonmukaista tarkastella kriisinhallinnan teorioiden avulla. Pragmaattisella tasolla tämä tarkoittaa, että tietosuojatyössäkin tulee pyrkiä tunnistamaan rekisteröityjen oikeuksiin liittyviä heikkoja signaaleja ja varhaisia varoituksia, jotka voivat johtaa jonkinasteiseen poikkeamaan. Kun löydösten todennäköisyys ja vakavuus arvioidaan mahdollisimman aikaisessa vaiheessa, on poikkeamaan tai sen uhkaan mahdollista reagoida optimaalisilla resursseilla. Kriisinhallinnassa tällä ennaltaehkäisyä korostavalla periaatteella on saatu vaikuttavuudeltaan toivottuja tuloksia.

Tiukimmin asetusta tulkitaan hyvinkin tiukasti, puhtaasti juridisesta viitekehyksestä. Toisena tulkintana voidaan pitää teknis- taloudellista, riskilähtöistä ja liberaalimpaa asetuksen tulkintaa. Valtionhallinnossa tietosuojaan liittyvien roolien, vastuiden sekä velvoitteiden määrittelyistä näyttää myös olevan eriäviä näkemyksiä, jotka omalta osaltaan haastavat tietosuojatyön norminmukaisuutta.

Toiseksi Valtorin roolia tietosuojassa ei ole määritelty virallisesti, mikä on johtanut eri virastoissa varsin kirjaviin tulkintoihin siitä, mitä Valtorin tietosuojaan liittyviin tehtäviin tulisi kuulua. Myös toimittajien ja Valtorin vastuut ovat epäselvät.

Tutkimuksessa esille tulleita pilvipalveluiden tietosuojaan liittyviä ristiriitaisuuksia on syytä tarkastella organisaatioiden pilvitransformaation yhteydessä. Teknologiana ja investointina pilvipalvelut ovat erittäin houkutteleva IT-ratkaisu, ja samanaikaisesti tietosuoja-asetus kannustaa ottamaan käyttöön uutta teknologiaa. Toisaalta on ilmeistä, että rekisteröityjen oikeuksia ei kyetä ylläpitämään eksplisiittisesti tietosuoja-asetuksen vaatimusten mukaisesti vallitsevien lainsäädäntöjen eriäväisyyksien vuoksi sekä tietojenkäsittelijöiden epätasaisen tietosuojaymmärryksen takia.

Tavoitteena onkin löytää strukturoitu malli, jolla kontrolloidaan koko ekosysteemissä tapahtuvaa henkilötietojen käsittelyä rekisteröidyn oikeuksien näkökulmasta ja tietosuojan hallintamallin mukaisesti. Tämä ajatus vahvistaa vallitsevan käsityksen, että rekisteröidyn oikeudet tulee ottaa huomioon jo hankintojen suunnitteluvaiheessa ja sisällyttää myös hankintojen vaatimuksiin. Oletusarvoisen ja sisäänrakennetun tietosuojan viitekehyksestä tällainen toiminta täyttäisi proaktiivisuuden, ennaltaehkäisyn sekä läpinäkyvyyden kriteerit.

7.2 Valtorin tietosuojan kypsyystaso

Tutkimuksessa tehty havainto, ettei vastaajien tietosuojan kypsyystaso ole kaikilta osin vaatimustenmukainen, korreloi siihen, millaisena vastaajat pitävät tietosuojaan liittyvän informaation tarvettaan. Tietosuojan kypsyystasolla on myös syy-seuraussuhde siihen, voidaanko tiedolla johtamisen teoriaa hyödyntää tietosuojatyössä. Juurisyy siihen, miksi olemassa oleva informaatio ei kohtaa päätöksentekijöitä ymmärrettävällä tavalla, näyttää olevan tietosuojan alhainen kypsyystaso sekä Valtorissa että laajemmin valtionhallinnossa.

Tiedolla johtamisen teoriaa tulkitaan Valtorissa varsin laveasti tai sitä ei tunneta lainkaan. Haastattelujen perusteella voidaan todeta, että sama haaste on tunnistettavissa laajemminkin valtionhallinnossa. Tästä seuraa, että virastojen, myös Valtorin, kompetenssi tehdä tietosuojaan liittyviä päätöksiä tiedolla johtamisen teoriaa noudattaen ja näyttöön perustuvan tiedon perusteella on rajallista. Tämä näkyy mm. kohdeorganisaation strategisen johdon kyvyttömyytenä ennaltaehkäistä eritasoisia tietosuojapoikkeamia ja niiden uhkia saamansa informaation perusteella. Tällainen syyn ja seurauksen suhde vaikuttaa organisaation kykyyn hyödyntää tiedolla johtamista tietosuojatyössä.

Haastatteluissa esiin nousseet käytännön esimerkit sitovat teoreettisen tarkastelun todellisuuteen ja vahvistavat edellä kuvattua analyysia. Tutkimuksen tulokset antavat ymmärtää, ettei päätöksentekijöillä ole juurikaan kompetenssia varmistaa oletusarvoisen ja sisäänrakennetun tietosuojan toteutumista pilvipalveluissa käytössään olevan informaation perusteella. Tietosuoja-asiantuntijat

eivät myöskään välitä tietosuojatyössä muodostunutta informaatiota eri asiantuntijoille niin, että se tukisi päätöksentekoa vaikuttavasti.

Edellä kuvattu antaa selkeitä viitteitä, etteivät Valtorin tietosuojatyössä toteudu oletusarvoisen ja sisäänrakennetun tietosuojan periaatteet: proaktiivisuus, ennaltaehkäisy, läpinäkyvyys ja riskilähtöisyys.

Analyysien tulosten pohjalta on perusteltua kyseenalaistaa, kykenevätkö asiantuntijat Valtorissa sekä laajemmin valtionhallinnossa muodostamaan saamastaan informaatiosta sellaista tietoa, jota he voivat käyttää päätöksenteon pohjana. Tähän näyttävät vaikuttavan seuraavat keskeiset asiat: kykenevätkö asiantuntijat jäsentämään saatavilla olevaa informaatiota päätöksentekoa varten relevantiksi tiedoksi, onko organisaatiossa tarpeeksi tietosuojaosaamista, jotta tietojenkäsittely olisi rekisteröidyn oikeuksien kannalta vaatimustenmukaista, sekä onko saatavilla oleva informaatio validia ja relevanttia sitä tulkitsevalle. Näiden kysymysten jälkeen voidaan arvioida, saavatko asiantuntijat juuri heille päätöksentekoa varten merkityksellistä informaatiota.

Analyysin tulosten perusteella voidaan kyseenalaistaa, hyödynnetäänkö tuotettua informaatiota niin, että se vahvistaa tietosuojatyön normien noudattamista. Tutkimuksessa nousee myös selvästi esille, että eri toimijoiden on tarkoituksenmukaista noudattaa henkilötietojen käsittelyssä eri maiden lainsäädäntöjä tilanteen mukaan. Tämä johtaa siihen, että organisaatioissa tulee olla käytettävissä osaamista eri maiden toisistaan merkittävästikin poikkeavan tietosuojalainsäädännön tulkitsemiseen.

Tietosuoja tunnistetaan sekä Valtorissa että laajemmin valtionhallinnossa periaatetasolla merkitykselliseksi. Tietosuoja-asetus näyttää olevan virastoille käsitteenä tuttu, mutta se mielletään kuitenkin vaikeaksi juurruttaa osaksi toimintaa. Viraston koolla ja tietosuojan kypsyystasolla näyttää olevan korrelaatio. Suurimmilla virastoilla vaikuttaa olevan paremmat mahdollisuudet resursoida tietosuojaan, mikä näkyy suoraan tietosuojan kypsyystasossa. Tämä ei kuitenkaan suoraan heijastu siihen, että eri virastojen välillä vallitsisi yksimielisyys toimijoiden rooleista, vastuista ja velvoitteista. Tutkimuksen aineisto osoittaa, ettei EU:n tietosuoja-asetusta ja kansallista tietosuojalainsäädäntöä pidetä valtionhallinnossa normina.

Yksi syy sille tosiasialle, että lähes puolet tutkimukseen osallistuneista ei osannut ottaa kantaa tietosuojaan liittyviin väittämiin, lienee se, että asetus on kirjoitettu yleisluontoisesti. Asetus on jäsenvaltioiden yhteisesti hyväksymä kompromissi, johon on jätetty paljon kansallista liikkumavaraa. Tämä johtaa erilaisiin tulkintoihin henkilötietojen käsittelyssä.

Haastatteluissa tuli ilmi, että useampi virasto tunnustaa olevansa liian pieni toimija neuvottelemaan pilvipalveluiden sopimusehdoista toimittajien kanssa. Näyttää kuitenkin siltä, että globaalit pilvipalveluiden toimittajat neuvottelevat henkilötietojen käsittelyyn liittyvistä ehdoista mieluummin erikseen jokaisen jäsenmaan sisällä eri toimijoiden kanssa kuin EU-tasolla. Valitun strategian taustalla saattaa yksinkertaisesti olla globaalien toimijoiden markkina-asema, joka on johtanut ns. vendor lock-in-tilanteeseen, jossa asiakkaan on vaikea vaihtaa palvelun toimittajaa.

Tutkimus osoittaa, ettei Valtorissa tietosuojan ja tietoturvan välinen vuorovaikutus ole kitkatonta, päinvastoin ääritapauksessa saatetaan jopa ajatella, että tietosuoja haittaa tietoturvan toteutumista. Haastattelun analyysi vahvistaa, että tämä ilmiö on tunnistettavissa laajemminkin valtionhallinnossa: sekä Valtorin ja virastojen välillä, että myös eri virastojen sisällä. Huomio on merkityksellinen, sillä merkittävä osa tietosuojavaatimuksista toteutetaan hallinnollisilla, fyysisillä tai teknisillä tietoturvakontrolleilla. Asetelma tulee tunnistaa heikoksi signaaliksi epäsuotuisasta kehityksestä, joka muodostaa toiminnallisen konfliktin. Tilanne on purettavissa lisäämällä tietosuojatyön läpinäkyvyyttä sekä tiedon jakamisen kulttuuria.

Analysoituani aineistoa tiedolla johtamisen teorian avulla syntyi vaikutelma, että tietosuoja-asetus ja kansalliset tietosuojalait tunnetaan heikosti ja niitä koskeva informaatio näyttää kryptiseltä datamassalta. Datamassaa kuvattiin pikemminkin lisätyötä aiheuttavaksi rasitteeksi kuin päätöksentekoa helpottavaksi informaatioksi. Kun informaation avulla jalostettua uutta tietoa ei juurruteta käytännön prosesseihin, on olemassa ilmeinen riski, ettei rekisteröidyn oikeuksia huomioida vaaditulla tasolla arkityössä. Rekisteröidyn oikeuksien toteutuminen on tietosuoja-asetuksen ensisijainen tavoite.

8 POHDINTAA

8.1 Havaintoja analyysistä

Analyysin havainnoista on mahdollista muodostaa neljä megatrendiä, jotka jo nyt vaikuttavat tietosuojatyöhön. Mikäli näihin ei reagoida, on todennäköistä, että tietosuojan vaatimustenmukaisuus ei jatkossakaan tule toteutumaan vaaditulla tasolla.

Analyysin tulos osoittaa, etteivät Valtorista kyselyyn osallistuneet vastaajat osanneet ottaa kantaa kaikkiin tietosuojalainsäädäntöä koskeviin väittämiin. Analyysi sai vahvistusta haastattelututkimuksen tuloksista. Valtorin eri johtotasot tuntevat ja tulkitsevat tietosuoja-asetusta ja kansallisia tietosuojalakeja heikosti. Tulkinta on myös usein ristiriidassa pilvipalveluiden toimittajien kanssa. Myös EU-alueen ulkopuolella tapahtuva tietosuoja-asetuksen vaatimuksista poikkeava tietojenkäsittely sekä lisäsuojakeinojen käyttö näyttävät herättävän laajasti eriäviä tulkintoja laajemminkin valtionhallinnossa, mikä tarjoaa mahdollisuuden **valita asetuksen liberaali tai tiukka tulkinta**. Tämä voidaan nostaa yhdeksi tutkimuksen megatrendiksi.

Toiseksi tutkimuksen megatrendiksi voidaan nostaa **tietosuojan taksonomia**. Toisistaan poikkeava ymmärrys tietosuojasta ja toisistaan poikkeava henkilötietojen luokittelu johtavat siihen, etteivät osapuolet tunnista henkilötietotyyppejä samalla tavalla. Vallitseva tilanne johtaa merkittävään riskiin, ettei rekisteröityjen oikeuksien huomioiminen valtionhallinnossa toteudu vaatimustenmukaisesti. Tulkinnat tuleekin selventää jo suunnitteluvaiheessa, ennen palveluiden käyttöönottoa. Yhteisesti sovitun taksonomian kautta syntyy tarkempi käsitys, onko siirrettävä tieto asiakkaan järjestelmän tuottamaan dataa vai järjestelmän itsensä tuottamaa dataa. Tämä tieto on oleellista, sillä tietojenkäsittelysopimuksissa (DPA, Data Protection Addendum) määritellään näille tietotyypeille rekisterinpitäjyys. Rekisterinpitäjän vastuulla on määritellä käytettävät tietoturvakontrollit vaatimusten mukaisuuden varmistamiseksi.

Sekä vastaajien koulutustausta että tutkimukseen liittyvän tietoturvaspesifien kysymysten vastaukset tuovat esille, että Valtori perustietotekniikkaa valtionhallinnolle tarjoavana virastona tuntee erinomaisesti pilviteknologian tekniset toteutukset. Samanaikaisesti voidaan todeta, että pilviteknologian käyttöönottoprosessien toteutukset ovat teknologiaorientoituneita, jolloin vaatimusmäärittelyjä tarkastellaan ensisijaisesti teknisestä viitekehyksestä. Teknologian käyttöönottaja edeltävissä keskusteluissa loppukäyttäjien näkemykset ovat näyttäneet jääneen vähäiselle huomiolle, mikä on johtanut siiloihin teknologisten asiantuntijoiden ja substanssiosaajien välillä.

Tiedolla johtamisen teoria korostaa näkökulmaa, että on ymmärrettävä, mihin tarpeeseen teknologian käyttö vastaa. Ajattelumalli muuttaa käytännön näkökulmaa niin, että ongelman ratkaisua tarkastellaan käyttäjien tarpeiden näkökulmista. Ajattelua ohjaa pikemminkin muutosprosessi, jota tuetaan teknologian avulla, kuin pelkkä puhdas teknologinen viitekehys. Tietosuojatyössä esitetty tiedolla johtamiseen perustuva ajattelu näyttää toimivan poikkeuksellisen hyvin. Kun ymmärretään tavoite, voidaan määritellä mitä henkilötietoja tulee käyttää. Tämän jälkeen voidaan määritellä minimihenkilötietojen yhdistelmä, jota tarvitaan tavoitteeseen pääsemiseksi. Suunnittelun viimeisessä vaiheessa voidaan määritellä henkilötiedon käsittelyn elinkaari. Kuvatulla toimintamallilla saavutetaan oletusarvoinen ja sisäänrakennettu tietosuoja. Tämän perusteella tutkimuksen kolmanneksi megatrendiksi nousi **henkilötietojenkäsittelyn tarkastelun kokonaisvaltaisuus.**

Merkittävä osa kohdeorganisaation vastaajista piti tietosuojaosaamistaan joko hyvänä tai erinomaisena. Kyselytutkimuksen kokonaistulos osoittaa kuitenkin, ettei kohdeorganisaation tietosuojan kypsyystaso vastaa sille asetettuja vaatimuksia. Asiantuntijahaastattelut vahvistavat tämän tulkinnan. Tutkimus vahvisti sekä osaamisen että tiedon siiloutumisen, eivätkä toimijat saa käyttöönsä juuri heidän tarpeitaan vastaavaa, datasta ja heikoista signaaleista jalostettua informaatiota päätöksenteon tueksi. Käytännössä tämä johtaa epävarmuuteen vastuun kantamisessa eikä tue proaktiivista tietosuojatyötä, mikä omalta osaltaan vahvistaa tulkinnasta heikosta tietosuojan osaamistasosta.

Tutkimuksessa ei voitu varmentaa, että Valtorissa henkilötietojen käsittely pilvipalveluissa on tarkoituksenmukaista. Myöskään henkilötietojen käsittelyprosessin läpinäkyvyyttä sekä tietojen minimikäsittelyn toteutumista ja elinkaaren hallintaa ei voitu varmentaa. Voidaan siis tulkita, ettei vielä olla vaaditulla tietosuojan kypsyystasolla. Tämän perusteella voidaan tutkimuksen neljänneksi megatrendiksi nostaa **tietosuojan kypsyystason vaatimustenmukaisuus.** Megatrendejä käsitellään tarkemmin alaluvussa 8.2.2.

8.2 Suuntaviivoja tietosuojatyön selkeyttämiseen

Pilvipalvelut jatkavat kasvuaan, ja henkilötietojen suojaaminen tulee aina vain monimutkaisemmaksi ja tärkeämmäksi. Tutkimuksen teon aikana jäsentyi niin sanottu tietosuojatyön algoritmi, jonka avulla organisaatiot voivat tarkastella

omaa tietosuojaansa, hahmottaa sen eri osatekijöitä ja vaikutusketjuja sekä ottaa sen kehittämisessä käyttöön tiedolla johtamisen periaatteita. Algoritmi esitellään alaluvussa 8.2.1.

Lisäksi organisaatioiden on hyvä tiedostaa muutamia megatrendejä, linjauksia ja valintoja, jotka vaikuttavat tietosuojatyöhön jatkossa. Alaluvussa 8.2.2 luodaan lyhyt katsaus niistä neljään. Organisaatioiden tasolla on kiinnitettävä huomiota tietosuoja-asetusten tulkintatapojen – tiukan ja väljän – vaikutuksiin sekä siihen, kuinka paljon koulutukseen halutaan panostaa. Koko maailmaa taas koskevat kysymykset siitä, onnistutaanko tietosuojatyön terminologiaa yhdenmukaistamaan – mikä helpottaisi sopimusten tekemistä sekä eri lakien yhteen sovittamista – sekä mihin suuntaan pilvipalveluita ja tietoturvaa aiotaan kehittää: otetaanko teknisen viitekehyksen rinnalle myös muut olennaiset asiat, esimerkiksi ihminen ja hänen tietojensa suojaaminen.

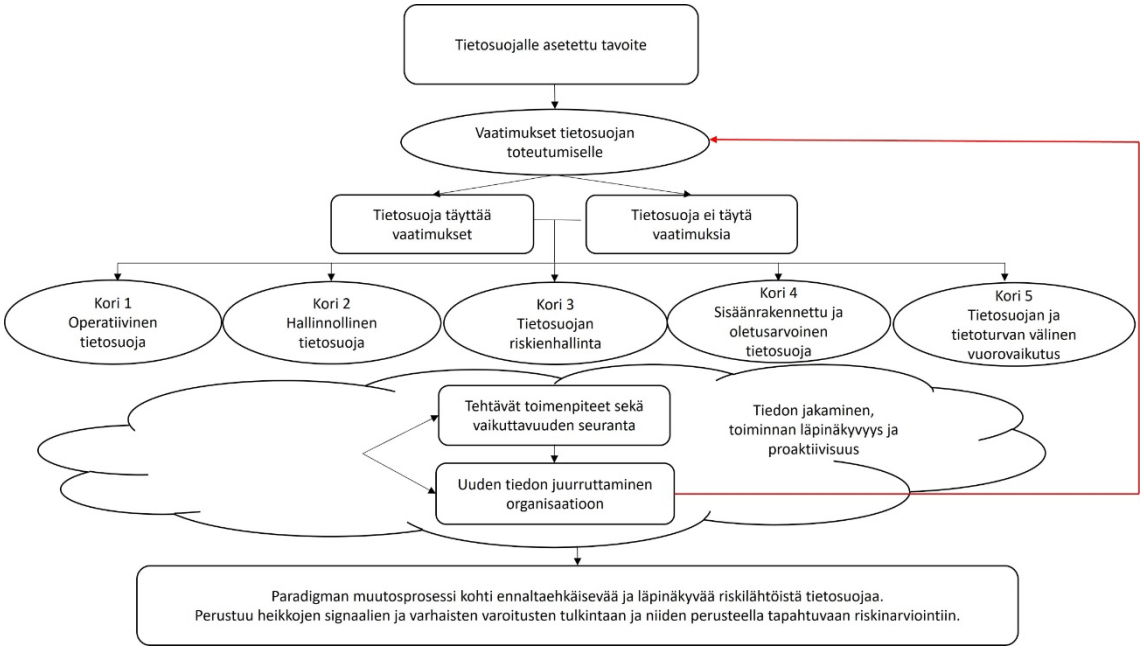
8.2.1 Tietosuojatyön algoritmi

Tietosuojatyön algoritmilla kuvataan askel askeleelta etenevää prosessia, joka on suunniteltu auttamaan tietosuojatyön liittyvien tehtävien suorittamisessa. Se on joukko selkeitä ohjeita tai sääntöjä, joita noudatetaan ongelmanratkaisun tai tietojenkäsittelyn aikana. Se on pragmaattinen kuvaus toimintamallista, joka ohjaa organisaatioita hyödyntämään tiedolla johtamisen periaatteita työssä, jossa tähdätään oletusarvoiseen ja sisäänrakennettuun tietosuojaan pilvipalveluissa (kuvio 18). Algoritmi alkoi hahmottua sitä mukaa kun tutkimusaineiston analysointi eteni. Pyrin systemaattisesti hakemaan tiedolla johtamisen kautta ratkaisuja tutkimuksessa esiin nousseisiin ongelmiin. Tämä prosessi jatkui niin kauan, kunnes sain vahvistuksen näkemykselleni, että syntynyt tietosuojatyön algoritmi auttaa ratkaisemaan tutkimuksessa esiin nousseita kysymyksiä.

Tietosuojatyön algoritmin tarkoituksena on luotsata henkilötietojen käsittelyprosessia systemaattisesti sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamiseen, jotta tietosuojan vaatimusten toteutuminen pilvipalveluissa voidaan varmistaa. Tämän lisäksi tavoitellaan myös kaikkien toimijoiden hyväksyttävissä olevaa, yhtenäistä tapaa jäsentää tietosuojaan liittyviä vaatimuksia sekä saada yhdenmukainen tulkinta eri toimijoiden rooleista, vastuista ja velvoitteista. Edellä kuvattu auttaa hahmottamaan tietosuojan vaatimuksia pilviteknologiassa ja ymmärtämään, mitä tietosuojaan liittyvää informaatiota eri toimijat tarvitsevat tietosuojatyön tueksi.

Algoritmilla pyritään lisäämään tiedon jakamisen kulttuuria sitä tarvitsevien asiantuntijoiden kesken, minkä tuloksena asiantuntijat saavat heille merkityksellistä informaatiota päätöksenteon pohjaksi.

Tietosuojatyön algoritmin avulla tietosuojatyössä pyritään paradigman muutokseen, jossa tavoitellaan proaktiivisesti riskiperusteista ja riskejä ennaltaehkäisevää henkilötietojen käsittelyä varmistamaan rekisteröityjen oikeuksien toteutuminen. Tähän tarvitaan näyttöön perustuvaa tietoa sekä ymmärrystä ja kykyä tulkita saatavissa olevaa informaatiota.



KUVIO 18. Tietosuojatyön algoritmi

Tietosuojatyön algoritmin ensimmäisessä vaiheessa organisaatioissa tunnistetaan, millaisia ovat tietosuojaa koskevat tavoitteet eli millaista tietosuojaa organisaatio tarvitsee pilvipalveluihinsa. Rooli perustietotekniikkaa tarjoavana palvelukeskuksena asettaa Valtorille poikkeuksellisia vaatimuksia tietosuojan toteuttamiseksi, koska se toimii paitsi oman toimintansa henkilötietojen rekisterinpitäjänä myös useiden muiden rekisterinpitäjien tietojenkäsittelijänä. Tämän lisäksi Valtorin turvallisuusyksiköllä (TUVE-yksikkö) on merkittävä määrä muita kansallisia lakisääteisiä velvoitteita, minkä vuoksi virastoilla on henkilötietojensa käsittelyyn varsin rajalliset vaikutusmahdollisuudet. Palvelukeskus-käsitettä ei mainita EU:n tietosuoja-asetuksessa, eikä siinä myöskään ole mainintaa kyseisestä roolista henkilötietojen käsittelyn yhteydessä. Tämä seikka, viranomaisten näkökulmasta puute, tuo omat haasteensa tavoitteen asetteluun.

Viranomaisen ydintehtävät ja tietojenkäsittely on määritelty kansallisessa lainsäädännössä: henkilötietojen käsittelyn tulisi olla selkeästi kuvattu ja käsittelyn käyttötarkoitussidonnaisuus tulisi olla ymmärretty. Tästä voidaan johtaa Valtorille lainsäädäntöön perustuva tavoite: varmistaa rekisteröityjen oikeuksien toteutuminen sekä varmentaa tietojenkäsittelyn vaatimustenmukaisuus luomalla valtionhallinnon vaatimukset täyttävä ja kustannustehokas tietosuojan hallintamalli. Toimenpiteiden vaikuttavuudella voidaan vaikuttaa positiivisesti siihen, miten julkishallinto siirtyy käyttämään pilvipalveluita.

Tavoitteen asettelussa tulee ottaa huomioon sisäänrakennettu ja oletusarvoinen tietosuoja jo henkilötietojen käsittelyn suunnitteluvaiheessa sekä palveluiden hankintaprosesseissa. Euroopan tietosuojaneuvosto kehottaa riskiperusteiseen ja ennakoivaan lähestymistapaan. Tietosuojaa on toteutettava tehokkaasti, ja rekisterinpitäjän odotetaan pysyvän ajan tasalla uusimmasta teknologiasta voidakseen taata jatkuvan tehokkaan tietosuojan. Rekisterinpitäjän tulee ottaa huomioon myös toteuttamiskustannukset. Näihin kysymyksiin vaikutetaan

huomioimalla uusin teknologia, kustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Tietosuojatyön algoritmissa tavoitteen asettamisen jälkeen organisaatiot määrittelevät kaikki vaatimukset, joiden tulee toteutua tavoitteeseen pääsemiseksi. Tässä työssä vaatimusten kokoamisen pohjana käytettiin EU:n tietosuoja-asetusta sekä kansallisia tietosuojalainsäädäntöjä. Algoritmin mukainen prosessi jatkuu siten, että vaatimuksista erotetaan ne osatekijät, jotka jo täyttyvät organisaatiossa, ja ne, jotka eivät täyty, minkä jälkeen voidaan keskittyä ratkaisemaan ne haasteet, jotka eivät vastaa vaatimuksiin.

Julkisesti käydyssä tietosuojakeskustelussa painotetaan voimakkaasti tarvetta päivittää pilvipalvelutoimittajien käyttöehtosopimuksia niin, että ne vastaavat paremmin EU:n tietosuoja-asetuksen vaatimuksiin. Keskustelussa jätetään kuitenkin huomioimatta, että käyttöehtosopimusten taustalla toimivat globaalit prosessit ja sopimusehtojen muuttaminen tarkoittaa sitä, että muutokset vaikuttavat globaalisti pilvipalveluihin. Merkittävä osa pilvipalveluiden käyttäjistä toimii EU:n tietosuoja-asetuksen vaikutusalueen ulkopuolella, joten ymmärrettävästi nämä sopimusneuvottelut ovat olleet usealle EU-jäsenvaltiolle melkeinpä ylitsepääsemätön haaste. Ongelman ratkaisua voidaan kuitenkin lähestyä holistisesti hallintamallin avulla pohtimalla, miten hallintamallin muiden osa-alueiden kautta voidaan päästä kaikkia osapuolia tyydyttäviin ratkaisuihin etsimällä riskeille kompensoivia kontrolleja muuttamatta välttämättä globaaleja sopimuksia.

Tässä tutkimuksessa vaatimustenmukaisuuden kriteerien katsottiin täyttyneen silloin, kun väittämien vastausten keskiarvo oli suurempi kuin 3,7 asteikolla yhdestä viiteen. Vaatimustenmukaisuuden kriteerit eivät täyttyneet väittämien keskiarvon jäädessä alle 2,5:n. Tämän tutkimuksen erityispiirteenä voidaan pitää sitä, että noin puolet väittämistä sai arvon noin 3, joka vastaa käytetyllä asteikolla ilmausta ”en ole samaa tai eri mieltä”. Tulos on tulkittava niin, etteivät vastaajat ole osanneet ottaa kantaa näihin väitteisiin. Näiden vastausten runsaus tuntuu poikkeukselliselta ja merkitykselliseltä sekä vahvistaa käsitystä, ettei tietosuojaosaaminen täytä tietosuojatyölle asetettuja vaatimuksia. Tulkinta vahvistui analysoitaessa ulkopuolisten asiantuntijoiden haastatteluaineistoja.

Seuraavassa vaiheessa vaatimukset jaetaan viiteen eri koriin. Kuvauksessa käytetään esimerkkinä Valtorin tietosuojan hallintamallia, ja korit on nimetty hallintamallin mukaisesti hallinnolliseen tietosuojaan, operatiiviseen tietosuojaan, tietosuojan riskienhallintaan, tietosuojan ja tietoturvan väliseen kytkökseen eli vuorovaikutukseen sekä oletusarvoiseen ja sisäänrakennettuun tietosuojaan.

Koreissa määritellään yksityiskohtaisesti näyttöön perustuvat toimenpiteet ja mittarit niille toimenpiteille, joita tarvitaan vaatimuksenmukaisuuden aikaansaamiseksi. Korit pitävät sisällään ne väittämäkohtaiset toimenpiteet, joilla vaikutetaan positiivisesti organisaation tietosuojan kypsyystasoon. Samalla määritellään tehtävälle toimenpiteelle aikataulu ja luodaan mittari, jonka avulla arvioidaan toimenpiteen vaikutusta tietosuojan kypsyystasoon. Toimenpiteiden tulee olla systemaattisia, näyttöön perustuvia, eksplisiittisiä ja hiljaista tietoa

hyödyntäviä. Kun kypsyys nousee vaaditulle tasolle, voidaan odottaa toimijoiden hyödyntävän tietosuojatyössä syntynyttä informaatiota tiedolla johtamisen teorian avulla.

Koreissa kuvatuilla toimenpiteillä ja mittareilla varmistetaan ja osoitetaan, että tietosuojaa toteutetaan teknisillä ja organisatorisilla toimenpiteillä, jotka voivat olla mitä tahansa hallinnollisia, fyysisiä tai teknisiä tietoturvakontrolleja – kaikkea kehittyneistä teknologiaratkaisuista henkilöstön perustasoiseen tietosuojakoulutukseen. Keskeistä on, että toiminnan vaikuttavuus pystytään todentamaan siten, että rekisteröidyn oikeudet toteutuvat rekisterinpitäjän määritysten mukaisesti. Rekisterinpitäjän tulee kyetä näyttöön perustuen osoittamaan rekisteröidyille ja viranomaisille, että henkilötietojen käsittely täyttää henkilötietojen käsittelyn käyttösidonnaisuuden ja minimikäsittelyn sekä tiedon elinkaaren hallintaan liittyvät vaatimukset. Käytännössä tämä tarkoittaa esimerkiksi pilvipalvelussa implementoituja tietoturva-asetuksia, joiden tulee tehokkaasti toteuttaa osaltaan tietosuojaa koko käsittelytoimessa. Kuvatussa esimerkissä toteutuu tietosuojan ja tietoturvan välinen vuorovaikutus. Näyttö taas syntyy esimerkiksi kolmansien osapuolten toteuttamien arviointien kautta.

Tietosuojatyön algoritmi tuo oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamiseen systemaattisen ja kattavan toimintatavan, jossa riskilähtöisyys on avaintekijä. Tarkasteltaessa kriisinhallintaa laajemmin voidaan todeta, että vaikuttavinta toimintaa poikkeamatilanteiden haltuunotossa on ennaltaehkäisy. On siis perusteltua kiinnittää ennaltaehkäisevään toimintaan huomiota myös tietosuojatyössä. Käytännössä tämä vaatii kykyä tunnistaa heikkoja signaaleja sekä varhaisia varoituksia ja kykyä arvioida rekisteröityjen oikeuksiin kohdistuvien riskien todennäköisyyttä. Toteutuakseen tämäkin vaatii organisaatiolta korkeaa tietosuojan kypsyystasoa.

Tiedolla johtaminen on kaikkea lyhyen ja hektisen toiminnan sekä pitkäkestoisen suunnittelun ja seurannan väliltä. Hektisimmillään se on suoraviivaista ja reaktiivista vaikuttamista poikkeamiin tai niiden uhkiin. Vaikuttamisen tulee tällöinkin olla riskilähtöistä ja ennakoivaa ja perustua heikkojen signaalien ja varhaisten varoitusten tunnistamiseen ja näiden perusteella riskin toteutumisen todennäköisyyden arvioimiseen. Algoritmin käyttäminen muuttaa aiemmin käytössä ollutta toimintamallia, jossa poikkeamiin tai niiden uhkiin on reagoitu reaktiivisesti, ei proaktiivisesti, johon kuitenkin tulee pyrkiä. Pitkäkestoisimmillaan tietosuojatyön tiedolla johtaminen on jopa vuosien ajan kestävää kokonaisvaltaista ja monipuolista, useiden asiantuntijoiden tekemää datan keruuta ja analysointia sekä uuden tiedon kerryttämistä, jakamista ja juurruttamista käytäntöön.

Tietosuojatyön algoritmissa uutta tietoa synnytetään, juurrutetaan ja jaetaan hyödyntämällä aiemmin kuvattua tiedolla johtamisen SECI-mallia. SECI-malli ei noussut esille tutkimuksen aikana käydyissä keskusteluissa – siitä voitaneen päätellä, ettei tätä tiedolla johtamisen osa-aluetta käytetä hyväksi tietosuojatyön strategisessa johtamisessa.

Tietosuojatyön algoritmissa läpinäkyvyyden vaatimus konkretisoituu siinä, että tiedon jakamisen kulttuuria vahvistetaan. Tavoitteena on, että

asiakkaan Valtorilta tilaama teknologia tukee asiakkaan lakisääteisten tehtävien toteutumista mahdollisimman tehokkaasti. Jotta tähän päästään, vaaditaan Valtorilta usein useamman teknisen ratkaisun integroimista. Valtorissa asiakaspalvelu on kuitenkin useimmiten nähty yksittäisten teknisten järjestelmien toimittamiseksi, jotka yhdistyvät asiakkaalla yhdeksi kokonaisuudeksi. Vallitsevassa tilanteessa onkin helppo nähdä, että tieto voi Valtorissa siiloutua, mikäli teknisistä järjestelmistä vastaavat asiantuntijat sekä asiakaspalvelusta vastaavat henkilöt eivät jaa tietoa keskenään ja asiakkaiden kanssa. Kuvattu ilmiö nousee esille jossain määrin aineiston analyysissä. Teknisistä ratkaisuista ja palveluista vastaavat toimijat olettavat, ettei heidän vastuullaan olevissa järjestelmissä käsitellä henkilötietoja tai että vastuu käsittelyn vaatimustenmukaisuudesta lankeaa jollekin toiselle.

Tietosuojatyön läpinäkyvyyden kannalta onkin merkityksellistä ylläpitää jatkuvasti henkilötietojen tietovirtakuvausta, jossa kuvataan, miten henkilötiedot kulkevat järjestelmästä toiseen ja miten henkilötietoja käsitellään koko niiden elinkaaren ajan. Tietovirtakuvaukset ovat konkreettisia kuvauksia tiedon siirtojen tunnistamiseen ja kartoittamiseen. Kuvaus auttaa määrittelemään yksiselitteisesti eri toimijoiden roolit, vastuut ja velvoitteet henkilötietojen käsittelyssä. Tutkimustulosten perustella tämäkin on ollut epäselvää niin Valtorille kuin sen asiakkaille ja pilvipalvelun toimittajille, jotka toimivat prosessissa Valtorin alihankkijoina.

8.2.2 Esiin nousseet megatrendit ja linjavalintoja organisaatioiden tietosuojatyön vahvistamiseen

Tutkimuksen tulosten perusteella on nostettavissa esiin neljä megatrendiä, joilla on merkittävää vaikutusta siihen, täyttyvätkö tietosuojan vaatimukset valtionhallinnon käyttämissä pilvipalveluissa. Tietosuojatyön kehittymiseen vaikuttaa ensinnäkin se, miten organisaatiossa ja laajemmin yhteiskunnissa tulkitaan voimassa olevia tietosuoja-asetuksia: väljästi vai tiukasti. Kansainvälisten sopimusten tekemiseen ja yhteistyön ongelmien määrään taas vaikuttaa keskeisesti se, saadaanko tietosuojatyön terminologia yhteiseksi niin, että kaikki puhuvat samasta asiasta. Samoin keskeinen kysymys on, kehitetäänkö pilviteknologiaa ja tietoturvaa jatkossakin lähinnä teknologisesta viitekehyksestä vai saadaanko muutkin tärkeät näkökulmat holistisesti mukaan. Lisäksi organisaatiot vaikuttavat tietosuojatyönsä kehittymiseen sillä, kuinka vahvasti ne panostavat koulutukseen.

Seuraavia linjavalintoja on tehty:

1. Tietosuoja-asetuksen väljä tulkinta vs. sen tiukka tulkinta

Valtiovarainministeriö painottaa linjauksessaan, että valtion yhteisten pilvi- ja ekosysteemiratkaisujen tulee olla ensisijainen valinta, mikäli estäviä perusteita valinnalle ei ole. Pilvi- ja ekosysteemiratkaisut tulee tuottaa lähtökohtaisesti EU- ja ETA-alueilla, jolloin ne ovat niiden lainsäädännön piirissä. Euroopan komissio hyväksyi 10. heinäkuuta 2023 EU:n ja Yhdysvaltojen tietosuojan riittävyyttä koskevan päätöksen, jossa todetaan, että Yhdysvallat takaa EU:n tietosuojaan

verrattuna riittävän suojan tason henkilötiedoille siirrettäessä niitä EU:n ja Yhdysvaltojen väliseen tietosuojakehykseen osallistuville yhdysvaltalaisille yrityksille (European Commission 2023b). Tämä voimaanastunut päätös on toistaiseksi voimassa, täyttäen tietosuoja-asetuksen vaatimuksia teknis-taloudellisesta viitekehyksestä. Linjaus ohjaa liberaaliin tulkintaan, jossa korostetaan riskiperusteista päätöstä. Tällöin tukeudutaan lähtökohtaisesti vaikutustenarviointeihin perustuviin riskinarviointeihin. Käytännössä pilviteknologia on rakentunut pitkällä aikavälillä sellaisille teknisille ominaisuuksille, joissa ei osattu huomioida kaikkia tietosuoja-asetuksen vaatimuksia, ja se on johtanut ristiriitaan tietosuoja-asetuksen väljän ja tiukan tulkinnan välillä.

Usein tästä dilemmasta on käytetty esimerkkinä IP-osoitetta, joka on tietosuoja-asetuksessa määritelty yksilöiväksi henkilötiedoksi. Tällöin sen siirtäminen EU- ja ETA-alueiden ulkopuolelle on vastoin asetuksen vaatimuksia. Teknisestä viitekehyksestä tarkasteltuna Internetissä globaalisti toimivat pilvipalvelut kuitenkin tarvitsevat käyttöönsä IP-osoitteet, jotta pilvipalvelu ylipäätään toimii. Kuvattu tilanne on tyypillinen esimerkki konfliktista, joka ei ratkea tarkastelemalla sitä yhdestä näkökulmasta, esimerkiksi juridisesta, teknisestä tai vain riskienhallinnan näkökulmasta. Sen sijaan ongelmia on tarkasteltava holistisesti ja pyrittävä etsimään kaikkia osapuolia tyydyttäviä kompensoivia kontrolleja. Teknis-taloudellinen tulkinta voisi johtaa siihen, että organisaatiot käsittelisivät henkilötietoja helpommin ja joustavammin, mutta samalla henkilötietojen suoja heikentyisi. Pilvipalvelut on lähtökohtaisesti rakennettava niin, että ne mahdollistavat kaikilta osin ja palvelun eri osatekijät yhdistettynä lain velvoitteiden täyttämisen.

Toista ääripäätä edustaa tietosuojan tiukka tulkinta, jonka edustajina voidaan pitää tietosuojavaltuutetun toimistoa ja Euroopan tietosuojaneuvostoa. Tiukan, juridista näkökulmaa korostavan tulkinnan voidaan katsoa tarkoittavan, että henkilötietojen käsittelyä valvotaan hyvin tarkasti ja sääntöjä sovelletaan tiukasti. Tällainen tulkinta voi johtaa esimerkiksi siihen, että organisaatiot joutuvat investoimaan enemmän resursseja tietosuojaan liittyviin toimiin ja että sääntöjä rikkoville asetetaan tiukemmat sanktiot.

Eri toimijoiden tulkinnat tietosuoja-asetuksesta ja sitä täydentävästä kansallisesta lainsäädännöstä asettuvat johonkin kohtaan liberaalin ja tiukan tulkinnan välillä. Päätös näyttää riippuvan siitä, kuinka paljon painoarvoa annetaan teknis-taloudelliselle tai juridiselle viitekehykselle. Tietosuojavaatimukset asettavat henkilötietojen käsittelyyn kuitenkin tarkat määräykset, eikä tietosuoja-asetuksen ja sitä tukevan kansallisen lainsäädännön noudattaminen ole vapaaehtoista. Tulkinnan tulee olla aina perusteltua ja oikeasuhtaista, ja se tulisi tehdä huolellisesti ottaen huomioon tietosuoja-asetuksen tavoitteet ja periaatteet, jotta rekisteröityjen oikeudet toteutuvat.

2. Tietosuojan käsitteiden ja luokittelun yhdenmukaistaminen

Toimijat tarkastelevat tietosuojaa omista viitekehyksistään ja puhuvat sen myötä asioista eri käsitteillä ja käyttäen eri luokitteluja ja taksonomioita. Se johtaa osaoptimointiin, minkä vuoksi kenellekään ei muodostu kokonaiskuvaa siitä, miten henkilötietojen käsittelyn vaatimuksenmukaisuus säilyisi loogisena

kokonaisuutena läpi koko käsittelyn ketjun. Tällöin käsittelyprosesseihin jää ns. harmaita alueita, joissa ei ole yksimielistä käsitystä tai sopimusta rooleista, vastuista ja velvoitteista. Tästä syntyy eriäviä näkemyksiä myös henkilötietojen käsittelyn tarkoituksista ja keinoista.

Edellä kuvattu IP-osoitekysymys on myös esimerkki siitä, miten eri käsitteiden ja luokittelujen käyttö johtaa eriäviin tulkintoihin. Toimittajat ajattelevat IP-osoitteiden kuuluvan pääsääntöisesti luokkaan ”system generated data”, jossa käsittelyn keinoja kontrolloi palvelun tarjoaja. Asiakkaat taas tulkitsevat joissain tapauksissa IP-osoitteet diagnostiikkatiedoiksi, joiden käyttötarkoitusta kontrolloi asiakas. Lopputuloksena muodostuu eriävä näkemys siitä, kuka määrittelee kyseisten tietojen käsittelyn vaatimukset.

Henkilötietojen käsittelyssä tiedolla johtamiseen perustuva holistinen tarkastelu tietosuojan hallintamallin kautta tarjoaa mahdollisuuden pilkkoa tietojenkäsittelyprosessi pienempiin ja helpommin hallittaviin osiin. Hallintamalli tarjoaa keinon tuottaa eri alojen asiantuntijoille juuri heille merkityksellistä informaatiota näyttöön perustuvan tiedon muodostamiseksi niin, että tietosuojan osaalueet tulee huomioitua tietosuojatyössä vaatimustenmukaisuuden varmistamiseksi.

3. Henkilötietojen käsittelyn kokonaisvaltainen tarkastelu

Pilviteknologian suunnittelua ohjataan vahvasti teknisestä näkökulmasta, jolloin keskitytään pohtimaan, miten teknologiaa käytetään. Tämä lähestyminen tukee huonosti tietosuojan vaatimusten täyttymistä, sillä siinä ei välttämättä oteta huomioon käsittelyn luonnetta, laajuutta, asiayhteyttä ja tarkoitusta eikä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä.

Lisäksi pilvipalveluiden ketjuuntuminen eri toimijoiden kesken johtaa siihen, että rekisterinpitäjänä toimiva asiakas menettää tietojen tai niiden osien yksinomaisen kontrollin ja mahdollisuuden varmistaa tarvittavat toimenpiteet tietojen eheyden ja luottamuksellisuuden takaamiseksi ja tarkistaa, käsitelläänkö ja säilytetäänkö tietoja asianmukaisesti. (United Nations 2019.)

Tiedolla johtamisen teoriaa noudatettaessa on keskeistä pohtia, mitä ollaan muuttamassa. Henkilötietojen käsittelyssä tämä kysymyksenasettelu näyttää olevan merkityksellinen. Kun on selvillä, mihin tietojenkäsittelyn avulla pyritään, voidaan määritellä tiedon käyttötarkoitussidonnaisuus, tiedon minimikäsittely sekä elinkaaren hallinta. Substanssiosaajien ja teknisten asiantuntijoiden välisiä siiloja tulee purkaa tiedon jakamista lisäämällä, jotta muutosprosessien toteuttajina toimivat ihmiset ja jotta teknologian tehtävänä on tukea muutosprosesseja.

Pilvipalveluiden ketjuuntuminen eri toimijoiden kesken johtaa siihen, että rekisterinpitäjänä toimiva asiakas menettää tietojen tai niiden osien yksinomaisen kontrollin ja mahdollisuuden varmistaa tarvittavat toimenpiteet tietojen eheyden ja luottamuksellisuuden takaamiseksi tai tarkistaa, käsitelläänkö ja säilytetäänkö tietoja asianmukaisesti. (United Nations 2019.)

4. Tietosuojan kypsyystaso organisaatiossa – koulutus keskeisessä asemassa

Tiedolla johtamisen avulla tapahtuva tietosuojan kypsyystason vaatimuksenmukaisuuden varmentaminen kohdeorganisaatiossa vaatii enemmän ja selkeämpää

tietosuojakoulutusta sekä -viestintää. Koulutuksissa tulee korostaa niitä konkreettisia toimenpiteitä, joilla henkilötietojen käsittelyä koskevia sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita toteutetaan rekisteröidyn oikeuksia ja vapauksia kunnioittavalla tavalla.

Koulutuksen ja viestinnän tulee kohdistua niille toimijoille, joiden vastuulla on varmistaa, että prosesseissa käsitellään kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Velvollisuus koskee kerättyjen henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Koulutuksessa ja viestinnässä tulee varmistaa hallinnollisin, teknisin, riskiperusteisin keinoin, ettei henkilötietoja saateta rajoittamattoman henkilömäärän saataville, että henkilötietoja ei käsitellä ETA-alueen ulkopuolella sijaitsevilla palvelimilla (data in rest) eikä tietoihin avata teknistä pääsy-yhteyttä ETA-alueen ulkopuolisesta maasta (data in transfer). Lisäksi tulee hyödyntää tarvittaessa lisäsuojakeinoja, jotka täydentävät vakiolausekkeita. Näiden periaatteiden täytäntöönpanoa varten tulee suunnitella asianmukaiset tekniset ja organisatoriset toimenpiteet ennen palveluiden siirtämistä tuotantoympäristöön.

9 TUTKIMUKSEN LUOTETTAVUUS JA JATKOTUTKIMUSKOHTEET

9.1 Tutkimuksen luotettavuuden arviointi

Tässä tutkimuksessa hyödynnettiin määrällistä ja laadullista tutkimusotetta sekä hyödynnettiin erilaisia mittaus- ja analysointitapoja tutkimuksen luotettavuuden varmistamiseksi.

Tutkimuksen objektiivisuuden tavoitteena on puolueeton tutkimusprosessi ja puolueettomat tutkimustulokset (Alkula ym. 2002). Tutkimusprosessin ja tulosten puolueettomuutta edesauttavat tutkittavan ja tutkijan etäinen suhde prosessin aikana sekä tutkijan mahdollisimman vähäinen vaikutus kyselyllä tai haastattelulla saatuihin vastauksiin ja tutkimuksen tuloksiin (Vilkka 2007). Tätä taustaa vasten on ollut perusteltua hyödyntää sähköistä kyselymoottoria kyselylomakkeen lähettämiseen, raportointiin ja kerätyn datan analysointiin

Triangulaatio eli eri menetelmien tai teorioiden yhdistäminen mahdollistaa tutkittavan ilmiön kattavan tarkastelun (114–118; Ronkainen, Pehkonen, Lindblom-Ylänne & Paavilainen 2011, 90). Triangulaation neljästä päätyypistä hyödynnettiin tässä tutkimuksessa kahta: aineistotriangulaatiota sekä teoriatriangulaatiota (Flick 1998, 229). Aineistotriangulaation täyttymisen ehtona on, että tutkimuksessa käytetään useita eri aineistoja tutkittaessa samaa ilmiötä. Tässä tapauksessa aineistoa kerättiin sekä Valtorin kolmelta johtotasolta (strateginen johto, keskijohto, lähijohto) että valtion eri virastojen tietosuoja-asiantuntijoilta. Teoriatriangulaation täyttymisen ehtona on, että tutkimusaineiston tulkinnassa käytetään useita teoreettisia näkökulmia. Tässä tapauksessa yhdistin useiden tieteenalojen teorioita, kuten tietojärjestelmätieteen, tiedolla johtamisen sekä kriisinhallinnan teorioita.

Reliabiliteetilla tarkoitetaan mittaustulosten toistettavuutta ja validiudella eli pätevyydellä sitä, että käsitteet mittaavat juuri tutkittavana olevaa asiaa (Heikkilä 2014, 29; Metsämuuronen 2011). Validiteetilla tarkoitetaan käytettyjen

menetelmien ja mittareiden kykyä tuottaa tuloksia, jotka antavat vastauksia esitettyihin tutkimuskysymyksiin.

Cronbachin alpha -kerroin ilmaisee mittarin sisäistä yhdenmukaisuutta (consistency) (Partala, 2009, 29), ja sillä voidaan määritellä summamuuttujiin latautuvat väittämät. Cronbachin alpha -kertoimen arvon suuruudesta, joka riittää edellisiin tarkoituksiin, on esitetty erilaisia näkemyksiä eri perustein. Metsämuuronen (2011) on esittänyt Cronbachin alpha -kertoimen hyväksyttäväksi alarajaksi 0,60. Vastaavasti Tähtinen ja Kaljonen (1996, 143) pitävät hyväksyttävänä alarajana arvoa 0,65. Alkula, Pöntinen ja Ylöstalo (2002, 99) ovat esittäneet arvoksi 0,70, ja Metsämuuronen (2011) pitää yhtäpitävyyttä hyvänä, jos arvo on yli 0,80. Nunnally (1978) arvioi alpha-kertoimen arvoa käyttötarkoituksen mukaan. Perustutkimuksessa arvon tulisi olla hieman yli 0,80, joka on vähän suurempi kuin hänen näkemyksensä yleisesti riittävästä alpha-kertoimen arvosta, joka on yli 0,70. Tässä tutkimuksessa yksittäisten väitteiden alpha-kertoimen arvot ovat 0,693–0,929. Hallintamallin osa-alueisiin alpha-kertoimet ovat yli 0,80, joten Nunnallyn (1978) perustutkimukseen asettama vaatimus alpha-kertoimen suuruudesta täyttyy.

Laadullisessa tutkimuksessa kysymykset tutkimuksen reliabiliteetista ja validiteetista on asetettava toisin kuin määrällisessä tutkimuksessa. Laadullisessa tutkimuksessa korostuvat analyysin systemaattisuuden ja tulkinnan luotettavuuden kriteerit. Tutkimuksen lukijalle osoitetaan, mistä aineisto koostuu, ja kuvataan aineiston osat, joiden varaan päähavainnot rakentuvat. Arvioitaessa tutkimuksen validiteettia mielenkiinto kohdistuu kerättyyn aineistoon ja niistä tehtävien tulkintojen johdonmukaisuuteen. (Ruusuvuori ym. 2011, 26–27; Heikkilä 2014.)

Luotettavuuden lisäämiseksi tutkimuksessa toteutettiin aineistotriangulaatio eli mukaan otettiin laadullinen osio, joka sisältää asiantuntijahaastatteluita. Haastateltaviksi valikoitui neljä satunnaisotannalla valittua valtionhallinnossa työskentelevää tietosuoja-asiantuntijaa. Lisäksi yhden ICT-palvelutalon asiantuntijoita haastateltiin ryhmähaastattelun menetelmin. Tutkimuksen validiteetin vahvistamiseksi haastatteluihin valituille asiantuntijoille asetettiin tarkat kriteerit.

Aineistotriangulaatio toteutettiin siten, että ensimmäisessä vaiheessa kerätyn aineiston analyysin tulokset alistettiin valikoitujen tietosuoja-asiantuntijoiden arvioitavaksi. Arvioitavana oli se, miten he itse kokevat väitteiden vastaavan tietosuojan kypsyystasoa Valtorissa. Samalla heitä pyydettiin arvioimaan väittämien suhdetta heidän oman organisaationsa tietosuojatyöhön. Analyysissä tarkastellaan, millaisena asiantuntijat pitivät Valtorin tietosuojan vaatimustenmukaisuutta sekä väittämäkohtaisia eroja valtion virastojen ja Valtorin välillä. Tulosten perusteella voidaan päätellä, kuinka normien mukaista toimintaa tietosuojatyö on, mikä käytännössä näkyy tietosuojaan liittyvien sääntöjen sekä määräyksien mukaisena ajatteluna ja toimintana valtionhallinnossa.

Tutkimus täyttää myös toistettavuuden vaatimuksen, koska se on toistettavissa eri valtion virastoissa. Toisto voidaan (ja tulisi) laajentaa koskemaan

laajempaa joukkoa valtion organisaatioita, koska kaikkien virastojen lakisääteisten tehtävien toteuttaminen vaatii henkilötietojen käsittelyä.

9.2 Mahdolliset jatkotutkimukset

Pilvipalveluiden turvallista käyttöä julkishallinnossa tulee tarkastella monesta näkökulmasta, hallinnollisesta, teknisestä sekä riskinhallinnan näkökulmista. Omasta näkökulmastaan tämä työ on alkua aiheesta tuotettavalle tiedolle ja toivottavasti innostaa käynnistämään uutta tutkimusta eri viitekehyksestä, jotta monimutkaisesta ja monikerroksisesta aiheesta saadaan mahdollisimman syvällistä näyttöön perustuvaa tietoa.

Tietosuoja on monimutkainen syiden ja seurausten verkosto, ja tässä tutkimuksessa on pyritty löytämään tärkeimmät vaikuttavat mekanismit päättelemällä saatujen vastausten perusteella niiden kausaalinen vaikutus. Tuloksia voitaneen käyttää katalysaattorina mahdollisille jatkotutkimuksille. Olisi syytä tutkia, ovatko analyysien tulokset yleistettävissä laajemmin EU-alueella ja olisiko esimerkiksi Bayes-mallinnus hyödyllinen, kun tutkitaan, minkä tietosuojan osa-alueen kehittäminen vaikuttaisi eniten siihen, että henkilötietojen vaatimustenmukaisuus toteutuu asetuksen ja lakien mukaisesti. Näitä tutkimalla avautuisi uusia mahdollisuuksia paradigman muutokselle kohti proaktiivista ja preventiivistä tietosuojatyötä.

Aiheen ympärillä on jo aloitettu uutta, syventävää tutkimusta. Vuoden 2022 aikana valtiovarainministeriö on käynnistänyt DigiFinlandin koordinoiman hankkeen, jonka tavoitteena on kartoittaa pilvipalvelutoimittajien sopimusehtojen päivittämisen perusteita tietosuojan viitekehyksestä ja vauhdittaa näin julkishallinnon siirtymistä pilvipalveluiden käyttöön. Hankkeen aikana on kartoitettu sopimusehtojen ristiriitaisuuksia julkishallinnon näkökulmasta. Hankkeen aikana on kartoitettu myös julkishallinnon tietosuojan kypsyystasoa rekisteröidyn oikeuksien toteutumisessa. Uutena löydöksenä nousi esille, että tietosuojakoulutusta olisi ohjattava pilvipalveluiden tietosuojan merkitykseen ja sisältöön. Mitä seuraamuksia voi syntyä, jos tätä aihetta ei tunneta eikä sitä oteta vakavasti? Mikäli tietosuojaa ei hallita, työskentely voi olla tehotonta, ja siitä voi seurata turhaa riskinottoa tai turhautumista koko tematiikkaan.

DigiFinlandinkaan tutkimuksessa vastauskäyttäytyminen ei ollut yhtenäistä. Kyselyn tuloksilla on siten merkitystä, kun pohditaan, miten tietosuojaa tulisi kehittää. Tutkimuksessa korostetaan, että kehittäminen vie oman aikansa eikä ongelmaan ole nopeita ratkaisuja. Tarvetta on selkeälle suunnitelmalle ja kehityksen seurantapisteille edistymisen tunnistamiseksi. Analyysissa nostetaan myös esille tiedolla johtaminen, joka on merkittävä asioiden näkyväksi tekemisen, syy-seuraussuhteiden löytämisen ja kehitystyön ohjaamisen kannalta.

Lopuksi teknologian kehitys kohti laajamittaista tekoälyn käyttöönottoa lisää eksponentiaalisesti datan käsittelyä, eittämättä myös henkilötietojen käsittelyä. Onkin ilmeistä, että mikäli tässä tutkimuksessa esiinnousseita teemoja ei

jatkossa huomioida, nousee myös riski rekisteröityjen oikeuksien ja vapauksien loukkauksille kasvamaan samassa suhteessa.

SUMMARY (YHTEENVETO)

To add value compared to previous studies, this research focuses on examining the phenomenon or privacy issues in cloud services from the perspective of knowledge management, a dimension that has not been extensively explored in previous studies on data privacy. The analysis in this study supports the research hypothesis: Knowledge management offers methods for a comprehensive examination of data privacy work. This is manifested through both the data privacy management model and the developed data privacy algorithm presented in this work. The findings correspond to the research question and present various models for enhancing the maturity level of data privacy, both within Valtori and more broadly in public administration.

The original study question revolves around the accessibility of information produced in data privacy work and the application of knowledge management theory in implementing Privacy by Design (PbD), which is one of the key requirements of the General Data Protection Regulation (GDPR). Given recent international debates, this question remains relevant. The analysis of this research was initiated with the interpretation of quantitative data, aiming to understand the information needs of different decision-makers and the available information supporting privacy by design implementation.

The research reveals data privacy challenges extending beyond Valtori to encompass public administration more largely. Decision-makers in public administration have access to information related to data privacy, aiding the implementation of cloud services in compliance with individuals' rights and privacy by design. However, the study concludes that the maturity level of data protection expertise across different leadership levels in the target organization falls short of meeting regulatory requirements. There is a divergence in understanding of data privacy among leadership levels.

Contrary to the study's hypothesis, it cannot be confirmed that leaders in various positions within the organization can acquire the necessary knowledge for compliant data privacy work based on the information they receive. The distribution of responses across the data privacy management model components reveals a significant portion of responses indicating indecision, suggesting a lack of clear opinions among respondents.

The study identifies a significant concern regarding the transfer of data from EU and EEA countries to third countries. This poses risks to data privacy requirements and may lead to potential non-compliance with regulations outside GDPR. The EU Court of Justice overturning the Privacy Shield arrangement in 2020 emphasizes the need for supplementary measures when transferring data to the United States. The responsibility for ensuring the adequacy of these measures lies with both the data controller and the data processor.

The interviews underscore challenges faced by agencies negotiating cloud service contracts, particularly with global providers. The market dominance of these providers contributes to a "vendor lock-in" situation, making it difficult for agencies to switch service providers. Differences in data protection legislation

between the EU and the United States exacerbate the challenges, as illustrated by the EU Commission's approval of the EU-U.S. Data Privacy Framework in 2023.

The study delves into the intersection of privacy and cybersecurity, revealing friction in this relationship. In some instances, data privacy is perceived to impede the realization of cybersecurity. The lack of consensus on data control standards and guidelines poses risks at the macro level, affecting data lifecycle, accessibility, usability, minimal data processing, usage dependency, resilience, and supplier dependence.

The study highlights the complexity and ambiguity surrounding the interpretation of GDPR. Conflicting practices emerge when stakeholders disagree on roles, responsibilities, and obligations related to personal data processing. This misalignment is observed in data processing agreements, leading to differing interpretations of terms between cloud service providers and the data protection regulation.

Interviews indicate a divergence in interpreting the GDPR, with different perspectives emerging based on the functional roles within government administration. The study identifies a correlation between agency size and data privacy maturity, with larger agencies demonstrating better resource allocation and maturity in data protection. However, this does not translate into unanimity on roles and responsibilities.

Respondents generally agree on the relevance of data privacy information for decision-making but express varying reactions to the regulation, leading to differences in how well data privacy work aligns with established norms. The study suggests a need for increased transparency in data privacy work and a culture of information sharing to address conflicts and foster understanding among stakeholders.

The study concludes that decision-makers at Valtori have access to data privacy information for implementing subjects' rights in cloud services. However, doubts arise about the effective utilization of this information to strengthen compliance with data privacy norms. The low maturity level of data protection at Valtori and across government administration is identified as a root cause hindering the meaningful integration of data privacy information into decision-making processes.

The study questions whether experts can effectively leverage information received for decision-making, emphasizing factors such as the ability to structure information, the organization's data privacy expertise, and the relevance of available information. The lack of clarity regarding which privacy-related information is relevant further contributes to uncertainty and challenges in implementing inherent and default data privacy.

In summary, the study reveals that decision-makers at Valtori have access to data privacy information, but challenges exist in effectively utilizing this information to ensure compliance with data privacy norms. The study underscores the need for increased clarity, transparency, and a unified approach to data privacy within government administration to address challenges and foster a culture of information sharing and compliance.

LÄHTEET

Aaltonen, M. (2009). Multi-ontology, sense-making and the emergence of the future. Futures, 41(5), 279–283.

Ackoff, R. (1989). From data to wisdom. Journal of Applied Systems Analysis, 16, 3–9.

Aden, H. (2020). Interoperability between EU policing and migration databases: Risks for privacy. European Public Law, 26(1).

Aho, M. (2011). Konstruktio suorituskyvyn johtamisen kypsyyden arviointiin. Väitöskirjatyö, Tampereen yliopisto.

Ahonen, O. (2020). Tiedolla johtaminen valtionhallinnossa: Valmiuksien ja maturiteetin arviointi. Pro gradu -tutkielma, Tampereen yliopisto.

Aktipis, M. S. & Katwan, R. B. (2021). Data protection commissioner v. Facebook Ireland Ltd. and Maximillian Schrems (CJEU). International Legal Materials, 60(1), 53–98.

Alasuutari, P. (2011). Laadullinen tutkimus 2.0. 4. painos. Vastapaino.

Ali, O., Shrestha, A., Chatfield, A. & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, 37(1), 101419.

Alkula, T., Pöntinen, S. & Ylöstalo, P. (2002). Sosiaalitutkimuksen kvantitatiiviset menetelmät. WSOY.

Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems. John Wiley & Sons.

Ansoff, I. (1975). Managing strategic surprise by response to weak signals. California management review 18.2., 21–33.

Ardichvili, A., Page, V. & Wentling, T. (2003). Motivation and barriers to participation in virtual knowledge-sharing communities of practice. Journal of knowledge management, 7(1), 64–77.

Asrar-ul-Haq, M. & Anwar, S. (2016). A systematic review of knowledge management and knowledge sharing: Trends, issues, and challenges. Cogent Business & Management, 3(1), 1127744.

Bali, R. K., Wickramasinghe, N., & Lehaney, B. (2009). Knowledge management primer. Routledge.

Barati, M., Aujla, G. S., Llanos, J. T., Duodu, K. A., Rana, O. F., Carr, M. & Ranjan, R. (2021). Privacy-aware cloud auditing for GDPR compliance verification in online healthcare. IEEE Transactions on Industrial Informatics, 18(7), 4808–4819.

Brenner, J. (2007). ISO 27001 risk management and compliance. Risk Management, 54(1), 24–29.

Bruma, L. M. (2020). An approach for information security risk assessment in cloud environments. Informatica Economica, 24(4), 29–40.

Bryman, A. (2004). Triangulation and measurement. Retrieved from Department of Social Sciences, Loughborough University, Loughborough, Leicestershire.

Brynjolfsson, E., Hitt, L. & Kim, H. (2011). Strength in numbers: How does data-driven decision making affect firm performance? SSRN Electronic Journal. http://doi.org/10.2139/ssrn.1819486
Calvi, A. (2022). Gender, data protection & the smart city: Exploring the role of DPIA in achieving equality goals. European Journal of Spatial Development, 19(3), 24–47.
Cavoukian, A. (2010). Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. Identity in the Information Society, 3(2), 247–251.
Chadwick, D. W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., ... & Wang, X. S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Generation Computer Systems, 102, 710–722.
Chenthara, S., Ahmed, K., Wang, H. & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access, 7, 74361–74382.
Christakis, T. (2019). Transfer of EU personal data to US law enforcement authorities after the CLOUD Act: Is there a conflict with the GDPR? In Cybersecurity and Privacy in a Globalized World - Building Common Approaches. New York University School of Law.
Creswell, J. W. & Clark, V. L. P. (2011). Designing and conducting mixed methods research. 2nd ed., Sage Publications, Thousand Oaks, CA.
Cummings, J. (2003). Knowledge sharing: A review of the literature. The World Bank Operations Evaluation Department.
Danescu, E. (2022). Viviane Reding on her action in the field of the information society and media (2004–2010). In Oral Histories of the Internet and the Web (pp. 109-122). Routledge.
Daskal, J. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Stanford Law Review online, 71, 9.
Deacon, D., Bryman, A., & Fenton N. (1998). Collision or collusion? A discussion and case study of the unplanned triangulation of quantitative and qualitative research methods. International Journal of Social Research Methodology, 1(1), 47–63.
Dinev, T. (2014). Why would we care about privacy? European Journal of Information Systems, 23, 97-102.
Dwivedi, A. N. (Ed.) (2009). Handbook of research on information technology management and clinical data administration in healthcare. IGI Global.
Dwivedi, A., Bali, R. K., James, A. E., Naguib, R. N. G., & Johnston, D. (2002). Towards a holistic knowledge management framework for healthcare institutions. In Proceedings of the Second Joint 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society. Engineering in Medicine and Biology, Vol. 3, pp. 1894–1895. IEEE.
EDPB (2020). Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf
Ekman, J. (2022). Katakri 2020 auditointityökalun osa-alue I:n hyödyntäminen arvioitaessa yrityksen teknistä tietoturvallisuutta. Opinnäytetyö, Laurea-ammattikorkeakoulu.
Eriksson, P. & Koistinen, K. (2014). Monenlainen tapaustutkimus. Kuluttajatutkimuskeskus.
Eskola, J. & Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. Vastapaino.
Euroopan unionin tuomioistuin (2020). Lehdistötiedote nro 91/20. Luxemburg
European Commission (2023a). Data protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flow. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.
European Commission (2023b). Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy framework. https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf
Flick, U. (1998). An introduction to qualitative research. Sage Publications.
Freshwater, D. & Cahill, J. (2013). Paradigms lost and paradigms regained. Journal of Mixed Methods Research 7, 3–5.
Frey, L., Botan, C. H., & Kreps, G. (2000). Investigating communication. Allyn & Bacon.
Furramani, E. & Ozpozan, N. K. (2023). Transfer of personal data to third countries and the "equivalent level" of protection according to the European Court of Justice. European Journal of Formal Sciences and Engineering, 6(1), 1–12.
George, D. A. S. & George, A. H. (2022). Potential risk: Hosting cloud services outside the country. International Journal of Advanced Research in Computer and Communication Engineering, 11(4), 5–11.
Gonzalez Fuster, G., Drechsler, L., Mahieu, R. & Nadolna Peeters, M. (2021). Feedback for the European Data Protection Board (EDPB) in response to the public consultation on 'Guidelines 10/2020 on restrictions under Article 23 GDPR Version 1.0 Adopted on 15 December 2020'
Gozman, D. & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. Journal of Business Research, 97, 235–256.
Guardian (2018). Privacy policies of tech giants 'still not GDPR-compliant'. https://www.theguardian.com/technology/2018/jul/05/privacy-policies-facebook-amazon-google-not-gdpr-compliant
Gupta, R., Gupta, I., Singh, A. K., Saxena, D. & Lee, C. N. (2023). An IoT-centric data protection method for preserving security and privacy in cloud. IEEE Systems Journal, 17(2), 2445–2454.

Gürsoy, G., Li, T., Liu, S., Ni, E., Brannon, C. M., & Gerstein, M. B. (2022). Functional genomics data: Privacy risk assessment and technological mitigation. Nature Reviews Genetics, 23(4), 245–258.
Haasio, A. (2015). Disnormatiivinen ja normatiivinen informaatio. Informaatiotutkimus, 34(4).
Hague Forum for Cloud Contracting (2019). European institutions convene to keep control over data processing in the cloud. https://slmmicrosoftrijk.nl/the-hague-forum-for-cloud-contracting/
Haikka, J. (2017). Johtamisen teoria: Ihmisen ja organisaation johtaminen. Diplomityö, Maasotakoulu.
Halonen, H. (2019). Ammatillisten oppilaitosten opettajien ja pk-yritysten henkilöstön välinen vuorovaikutus osaamisen hyödyntämisessä ja kehittämisessä. Väitöskirja, Tekniikan ja luonnontieteiden tiedekunta, Tampereen yliopisto.
Hannila, P. & Kyngäs, P. (2008). Teemahaastattelu laadullisessa tutkimuksessa. Opinnäytetyö, Helsingin ammattikorkeakoulu Stadia.
Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A. & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. Information Systems, 47, 98–115. https://doi.org/10.1016/j.is.2014.07.006.
Heikkilä, T. (2014). Tilastollinen tutkimus. 9. uudistettu painos, Edita.
Heino, P. (2010). Pilvipalvelut. Talentum.
Helin, M. (2021). Kohti EU:n omaa turvallista kybermaailmaa. Kandidaatintutkielma, Jyväskylän yliopisto.
Helsingin Sanomat (2013). Ulkoministeriön verkko oli täysin ulkopuolisten hallussa. https://www.hs.fi/kotimaa/art-2000002685298.html .
Hirsjärvi, S. & Hurme, H. (2008). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Gaudeamus.
Hokkanen, J. (2015). Yksityisyys ja yksityisyyden suojaaminen big datan aikakaudella: Teknologinen näkökulma. Kandidaatintutkielma, Jyväskylän yliopisto.
Hätilä, M. (2020). Tiedolla johtamisen mahdollisuudet ja haasteet kunnissa. Pro gradu -tutkielma, Tampereen yliopisto.
IBM (2012). Pilvipalvelut. http://www05.ibm.com/fi/solutions/cloud/services.html .
Iivari, J. (2023). Inductive empiricism, theory specialization and scientific idealization in IS theory building. Communications of the Association for Information Systems, 52, 910-914
Immonen, A., Bali, R. K., Naguib, R. N. G., & Ilvonen, K. (2009). Towards a knowledge-based conceptual model for post-crisis public health scenarios. In Proceedings of the IEEE International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (Manila, Philippines), pp. 185–189.

Immonen, A., Bali, R. K., & Wickramasinghe, N. (2008). Towards a knowledge-based secure healthcare resource balancing system. In AMCIS 2008 Proceedings. 112. https://aisel.aisnet.org/amcis2008/112.
Immonen A. & Rantanen, H. (2011). Informaatio- ja kommunikaatioteknologian liiketoimintamahdollisuudet kriisinhallinnassa. Pelastusopiston julkaisu, B-sarja: Tutkimusraportit 4/2011.
Immonen, A. & Rantanen, H. (2013). Sosiaalisessa mediassa syntyneen datan hyödyntäminen onnettomuuksissa ja muissa kriiseissä. Palotutkimuksen päivät 2013, 8–12. Palo- ja Pelastustieto ry.
Impiö, J. (2021). Yleisen tietosuoja-asetuksen vaatimusten toteuttaminen pk-yrityksessä. Opinnäytetyö, Laurea-ammattikorkeakoulu.
Iqbal, A. (2021). Innovation speed and quality in higher education institutions: the role of knowledge management enablers and knowledge sharing process. Journal of Knowledge Management, 25(9), 2334–2360.
Jalonen, H. (2015). Tiedolla johtamisen näyttämö ja kulissit. Teoksessa Tiedolla johtaminen hallinnossa: Teoriaa ja käytäntöjä, 40–68. Tampereen yliopistopaino Oy.
Javanainen, T. (2019). Jälkilaskennan kehittäminen valmistavan teollisuuden yrityksessä. Diplomityö, Tampereen yliopisto.
Johansson, A. (2022). EU:n yleisen tietosuoja-asetuksen mukainen turvallinen henkilötiedon siirto EU/ETA:n ulkopuolelle. Opinnäytetyö, Laurea-ammattikorkeakoulu.
Junttila, R. (2013). Lain asettamat vaatimukset henkilörekistereille ohjelmistoprojektissa. Opinnäytetyö, Oulun seudun ammattikorkeakoulu.
Järvinen, K. (2020). Tekoälyavusteisen päätöksenteon etiikan tarkastelu. Kandidaatintutkielma, Tampereen yliopisto.
Kaivola, T. (2016). Kehittyvät digitaaliset sisämarkkinat ja henkilötietojen suoja perusoikeutena. Pro gradu -tutkielma, Helsingin yliopisto.
Kaivo-oja, J. (2012). Weak signals analysis, knowledge management theory and systemic socio-cultural transitions. Futures, 44(3), 206–217.
Kaivo-oja, J. (2021). Kuinka tarkasti pystymme ennustamaan tulevaisuutta ja miten se tehdään? Plenaariesitelmä Sotatieteiden päivillä 3.–4.11.2021. Maanpuolustuskorkeakoulu ja Suomen Sotatieteellinen Seura ry.
Kakkori, L., & Huttunen, R. (2014). Fenomenologia, hermeneutiikka ja fenomenografinen tutkimus. Teoksessa Ajan kasvatus: Kasvatusfilosofia aikalaiskritiikkinä, 367-400. Tampere University Press.
Kanakia, H., Shenoy, G., & Shah, J. (2019). Cambridge analytica: A case study. Indian Journal of Science and Technology, 12(29), 1–5.
Karvi, T. (2010). Tietoturvan perusteet. Luku1: Yleistä tietoturvasta. https://dokumen.tips/documents/tietoturvan-perusteet-luku-1-yleistae-tietoturvasta.html?page=1
Kasanen, E., Lukka, K. & Siitonen, A. (1991). Konstruktiivinen tutkimusote liiketaloustieteissä. Liiketaloudellinen Aikakausikirja 3, 301–329.

Kataja, J. (2021). EU:n yleinen tietosuoja-asetus: Rekisteröidyn oikeuksien toteutuminen ja datanhallinnan hyödyntäminen yrityksissä. Pro gradu -tutkielma, Jyväskylän yliopisto.
Katzer, M. & Crawford, D. (2013). Office 365 compliance and data loss prevention. In Office 365: Migrating and Managing Your Business in the Cloud, pp. 429-481. Apress, Berkeley, CA.
Kaula, R. (2015). Business intelligence rationalization: A business rules approach. Business and Management 7(1), 129–143.
Kekkonen, J. (2008). Vertailevan tutkimuksen haasteita. Tieteessä tapahtuu, 26(3–4).
Kivekäs, R. (2014). Siilot organisaatiokulttuurisena ilmentymänä. Pro gradu -tutkielma, Lappeenrannan teknillinen yliopisto.
Kivinen, T. (2008). Tiedon ja osaamisen johtaminen terveydenhuollon organisaatioissa. Väitöskirja, Yhteiskuntatieteellinen tiedekunta, Kuopion yliopisto.
Kleemola, M. (1998). Terveystutkimuksen tietosuoja EU-Suomessa. Kansanterveyslaitoksen tiedotuslehti 1998(5), 3.
Koivuharju, O. (2013). Tietoturva järjestelmäkehityksessä. Metropolia Ammattikorkeakoulu.
Koivula, P. (2008). Johtaminen ja IT:n mahdollisuudet: Survey-tutkimus julkishallinnon johtajien käyttämistä IT:n mahdollisuuksista vuosina 1992 ja 2006. Väitöskirja, Tampereen yliopisto.
Koraeus, M. (2008). Who knows? The use of knowledge management in crisis. Förvarshögskolan, Stockholm.
Korhonen, R. (2003). Perusrekisterit ja tietosuoja. Edita.
Korpisaari, P., Pitkänen, O. P., & Warma-Lehtinen, E. (2018). Uusi tietosuojalainsäädäntö. Alma Talent.
Kosonen, J. (2015). Tietoturva pilvipalveluissa. Kandidaatin tutkielma, Jyväskylän yliopisto.
Kreiner, K., Immonen, A. & Suominen, H. (2013). Crisis management knowledge from social media. In ADCS '13: Proceedings of the 18th Australasian Document Computing Symposium, pp. 105–108. ACM.
Laakso, M. (2010). PK-yrityksen tietoturvasuunnitelman laatiminen. Opinnäytetyö, Turun ammattikorkeakoulu.
Laaksovirta, T. H. (1983). Tieteellinen ajattelu – arkiajattelu. Informaatiotutkimus, 2(1), 11–18.
Lachaud, E. (2020). ISO/IEC 27701 standard: Threats and opportunities for GDPR certification. European Data Protection Law Review, 6, 194.
Laudan, L. (1978). Progress and its problems: Towards a theory of scientific growth. University of California Press, Berkeley, CA.
Lehtinen, V. (2010). Tietoturvan ja tietosuojan kehittäminen pilviteknologiassa: Standardit ja kehysmallit sekä riskienhallinnan näkökulma. Pro gradu -tutkielma, Jyväskylän yliopisto.

Lehto, M. & Neittaanmäki, P. (2014). Informaatioteknologian tiedekunnan tutkimus- ja koulutusstrategia: White Paper. Informaatioteknologian tiedekunnan julkaisuja 18/2014. Jyväskylän yliopisto.
Lilleoere, A. M. & Holme Hansen, E. (2011). Knowledge-sharing enablers and barriers in pharmaceutical research and development. Journal of Knowledge Management 15(1), 53–70. http://doi.org/10.1108/13673271111108693.
Limnéll, J. (2014). Kyber rantautui Suomeen. Aalto-yliopiston julkaisusarja, 12/2014.
Liu, L., Chen, R., Liu, X., Su, J. & Qiao, L. (2020). Towards practical privacy-preserving decision tree training and evaluation in the cloud. IEEE Transactions on Information Forensics and Security, 15, 2914–2929.
Loisa, M. (2006). Uuden tiedon luominen ja skenaariomenetelmä. Kandidaatin tutkielma, Lappeenrannan-Lahden teknillinen yliopisto LUT.
Lukka, K. (2000). The key issues of applying the constructive approach to field research. In Reponen, T. (ed.), Management Expertise for the New Millenium, pp. 113–128. Turku School of Economics and Business Administration.
Lukka, K. (2006). Konstruktiivinen tutkimusote: Luonne, prosessi ja arviointi. Teoksessa K. Rolin, M. Kakkuri-Knuuttila, E. Henttonen & K. Eräranta (toim.), Soveltava yhteiskuntatiede ja filosofia, 111-133. Gaudeamus.
Lumijärvi, I. (2015). Tulosjohtaminen ja tuloksellisuuden tavoittelu. Teoksessa I. Karppi (toim.), Governance – Hallinnan uusia ulottuvuuksia, 74–79. Tampereen yliopisto.
Lähdesmäki, M. (2020). Tietoturvan ylläpitäminen julkisissa pilvialustoissa. Opinnäytetyö, Haaga-Helia-ammattikorkeakoulu.
Malinen, M. & Pyykkö, A. (2010). Julkishallinnon IT-kehityshankkeiden epäonnistuminen ja siihen johtavat syyt: Tapaustutkimus. Pro gradu -tutkielma, Jyväskylän yliopisto.
Malkamäki, K. (2017). Luottamuksen kehittyminen ja johtamisjärjestelmää koskeva uudistus: Tapaustutkimus kaupan alan organisaatiosta. Väitöskirja, Itä-Suomen yliopisto.
Mannermaa, M. (2004). Heikoista signaaleista vahva tulevaisuus. 2. painos, WSOY.
Marshall, A, Mueck, S., & Shockley, R. (2015). How leading organizations use big data and analytics to innovate. Strategy & Leadership 43(5), 32–39.
Markopoulou, D., Papakonstantinou, V. & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336.
Marr, B. (2010). The intelligent company: Five steps to success with evidence based management. John Wiley & Sons.
Matinmikko, J. (2020). Henkilötietojen hyödyntäminen kohdennetussa verkkomainonnassa. Kandidaatintyö, Lappeenrannan-Lahden teknillinen yliopisto LUT.

Matošková, J. (2016). Measuring knowledge. Journal of Competitiveness, 8(4), 5–29. https://doi.org/10.7441/joc.2016.04.01
Mattessich, R. (1995). Critique of accounting: Examination of the foundations and normative structure of an applied discipline. Bloomsbury Publishing.
McCarthy, J. (1961). A basis for a mathematical theory of computation, preliminary report. In Proceedings of the Western Joint Computer Conference, Papers presented at the Joint IRE-AIEE-ACM Computer Conference (Los Angeles, Calif., 1961), pp. 225–238.
Mell, P. & Grance, T. (2009). Perspectives on cloud computing and standards. National Institute of Standards and Technology (NIST).
Melto, M. (2019). EU-asetuksesta kansalliseen lainsäädäntöön: Tietosuojalaki. Opinnäytetyö, Laurea-ammattikorkeakoulu.
Metsämuuronen, J. (2002). Metodologian perusteet ihmistieteissä. International Methelp Oy.
Metsämuuronen, J. (2006). Laadullisen tutkimuksen käsikirja. International Methelp Oy.
Metsämuuronen, J. (2011). Tutkimuksen tekemisen perusteet ihmistieteissä. International Methelp Oy
Mi, H., Wang, H., Yin, G., Cai, H., Zhou, Q., Sun, T., & Zhou, Y. (2011). Magnifier: Online detection of performance problems in large-scale cloud computing systems. In 2011 IEEE International Conference on Services Computing, pp. 418–425. IEEE.
Moody, G., Siponen, M., Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly, 42(1), 285-311.
Morgan, G. & Smircich, L. (1980). The case for qualitative research. Academy of Management Review, 5(4), 491–500.
Muhren, W., Eede, G. V. D., & Walle, B. V. D. (2008). Sensemaking and implications for information systems design: Findings from the Democratic Republic of Congo's ongoing crisis. Information technology for development, 14(3), 197–212.
Mustonen, A. (2015). Euroopan parlamentin Suomen tiedotustoimiston kriisiviestintäsuunnitelma: Ennaltaehkäisyn merkitys kriisiviestinnässä. Opinnäytetyö, Haaga-Helia-ammattikorkeakoulu.
Natunen, A. (2014). Tiedon omistajuus pilvipalveluissa tietoturvan, lainsäädännön ja käyttöehtojen näkökulmasta.
Neilimo, K. & Näsi, J. (1980). Nomoteettinen tutkimusote ja suomalainen yrityksen taloustiede: Tutkimus positivismin soveltamisesta. Yrityksen taloustieteen ja yksityisoikeuden laitoksen julkaisuja, Sarja A 2, Tutkielmia ja raportteja. Tampereen yliopisto.
Niiniluoto, I. (1984). Johdatus tieteenfilosofiaan: Käsitteen- ja teorianmuodostus. Otava.
Niiniluoto, I. (1989). Informaatio, tieto ja yhteiskunta: Filosofinen käsiteanalyysi. Valtion painatuskeskus.

Nodehi, T., Ghimire, S., Jardim-Goncalves, R., & Grilo, A. (2013). On MDA-SOA based intercloud interoperability framework. Computational Methods in Social Sciences, 1(1), 5.
Nonaka, I. & Takeuchi, H. (1995). The knowledge-creating company: How Japanese companies create the dynamics of innovation. Oxford University Press.
Nunnally, J. C. (1978). Psychometric theory. McGraw-Hill.
Nyst, C. & Falchetta, T. (2017). The right to privacy in the digital age. Journal of Human Rights Practice, 9(1), 104–118.
Närhinen, I. (2022). EU: n yleisen tietosuoja-asetuksen käyttöönoton tukemisen keinoja pienyrityksessä (case ICT-palveluntuottaja Järvi-Suomen Kiinteistökonsultit Oy). Pro gradu -tutkielma, Jyväskylän yliopisto.
Oksman, M. (2017). Naisjohtajien käsityksiä innovatiivisuudesta: Tapaustutkimus kolmesta naisjohtajasta. Pro gradu -tutkielma, Itä-Suomen yliopisto.
Paajanen, E. (2017). Tietosuoja-asetuksen vaikutukset organisaatioihin ja Amazon Web Services -pilvipalvelualustan tuoman hyödyt. Diplomityö, Lappeenrannan teknillinen korkeakoulu.
Pakkala, E. (2021). Selvitys: Vastaamo laiminlöi lukuisia velvollisuuksiaan – potilastiedoissa sinne kuulumattomia tietoja. https://www.uusisuomi.fi/uutiset/selvitys-vastaamo-laiminloi-lukuisia-velvollisuuksiaan-potilastiedoissa-sinne-kuulumattomia-tietoja/c7bbbbe1-4472-448c-9666-fa2dbf40fdb1
Paloniemi, S. (2004). Ikä, kokemus ja osaaminen työelämässä: Työntekijöiden käsityksiä iän ja kokemuksen merkityksestä ammatillisessa osaamisessa ja sen kehittämisessä. Väitöskirja, Jyväskylän yliopisto.
Parkkila, L. (2013). Hiljaisen tiedon keräämisen ja konkretisoinnin toimintamallit: IMTAC-hankkeen kirjallisuustutkimus. Kemi-Tornion ammattikorkeakoulun julkaisuja, sarja B, Raportit ja selvitykset 16/2013. Kemi–Tornion ammattikorkeakoulu.
Partala, A.-E. (2009). Fyysisen aktiivisuuden ja toimintakyvyn yhteys ikääntyneiden hyvinvointiin Suomessa. Pro gradu -tutkielma, Jyväskylän yliopisto.
Pervez, Z., Lee, S. & Lee, Y.-K. (2010). Multi-tenant, secure, load disseminated SaaS architecture. In 2010 The 12th International Conference on Advanced Communication Technology (ICACT), pp. 214–219. IEEE.
Pohjalainen, H. (2018). GDPR ja sen vertaaminen Yhdysvaltojen tietosuojasääntelyyn. Opinnäytetyö, Turun ammattikorkeakoulu.
Pohjalainen, M. (2016). Hiljaisen tiedon tunnistaminen, jakaminen ja uuden tiedon luominen kirjastotyön kontekstissa. Väitöskirja, Tampereen yliopisto.
Puhakka, R. (2021). Tietomurtojen vaikutus internetin käyttäjien tunteisiin ja käytökseen. Pro gradu -tutkielma, Jyväskylän yliopisto.
Purnaye, P. & Kulkarni, V. (2022). A comprehensive study of cloud forensics. Archives of Computational Methods in Engineering, 29(1), 33–46.

Päivelin, J. (2019). Oleellisimmat vaatimukset ICT-yritykselle tietoturvallisuuden toteuttamiseksi. Insinöörityö, Metropolia-ammattikorkeakoulu.
Raavo, J. (2021). Tiedolla johtaminen kansainvälisessä yrityksessä. Opinnäytetyö, Haaga-Helia-ammattikorkeakoulu.
Raj, P. (2013). Cloud Enterprise Architecture. Taylor & Francis, Boca Raton, FL.
Ralston, W. (2020). A dying man, a therapist and the ransom raid that shook the world. WIRED UK. Haettu 3.5.2020. https://www.wired.co.uk/article/finland-mental-health-data-breach.
Raman, M., Ryan, T., & Olfman, L. (2006). Knowledge management systems for emergency preparedness: The Claremont University Consortium experience. International Journal of Knowledge Management (IJKM), 2(3), 33–50.
Rautiainen, P. (2021). Henkilötietojen siirto EU: sta Yhdysvaltoihin ja rekisterinpitäjän lisäsuojatoimenpiteet. Pro gradu -tutkielma, Tampereen yliopisto
Razdan, V. (2013). Contours of right to privacy. International Journal of Management, IT and Engineering, 3(11), 456–468.
Reponen, T. (2021). Pilvipalveluiden lakitekniset rajoitteet ja käytänteet: Julkinen sektori. Pro gradu -tutkielma, Jyväskylän yliopisto.
Richards, N. M., & Solove, D. J. (2007). Privacy's other path: Recovering the law of confidentiality. Georgetown Law Journal, 96, 123–182.
Ronkainen, S., Pehkonen, L., Lindblom-Ylänne, S. & Paavilainen, E. (2011). Tutkimuksen voimasanat. WSOYpro.
Ruusuvuori, J., Nikander P. & Hyvärinen, M. (2011). Haastattelun analyysin vaiheet. Teoksessa J. Ruusuvuori, P. Nikander & M. Hyvärinen (toim.), Haastattelun analyysi, 9–26. Vastapaino.
Ryan-Mosley, T. (2023). A controversial US surveillance program is up for renewal. Critics are speaking out. MIT technology Review.
Rydenfelt, H. (2014). Eettinen ennakointi. ProComma Academic, 40–47.
Rönkkö, I., Kinnunen, U. M., Kiviharju, S. & Mäkinen, R. (2016). Potilastiedot hyötykäyttöön perusterveydenhuollossa – tarvitaan kysymisen taitoa, dataa ja tiedonlouhinnan osaamista. Finnish Journal of eHealth and eWelfare, 8(1), 14–29.
Salmio, P. (2012). Pilvipalvelut. Opinnäytetyö, Turun Ammattikorkeakoulu.
Sanastokeskus (2019). Tepa-termipankki. Sv. pilvipalvelut. https://termipankki.fi/tepa/fi/haku/pilvipalvelu.
Sandfuchs, B. (2021). The future of data transfers to third countries in light of the CJEU's Judgment C-311/18 – Schrems II. GRUR International, 70(3), 245–249.
Saumya, C. (2015). Enterprise information management in practice: Managing data and leveraging profits in today's complex business environment. Springer.
Saunders, M., Lewis, P. & Thornhill, A. (2009). Research methods for business students. 5th edition, Prentice Hall.

Savolainen, R. (1994). Tiedon käytön tutkimus informaatiotutkimuksessa. Informaatiotutkimus, 13(4), 101–119.
Sharma, T., Wang, T., Di Giulio, C. & Bashir, M. (2020). Towards inclusive privacy protections in the cloud. In Applied Cryptography and Network Security Workshops – ACNS 2020, pp. 337–359. Springer.
Siikaniemi, L. (2005). Magnetic metal: Toward a model for satisfaction of education and career in vocational upper secondary education and training of machinery and metal technology in the Lahti region. Tampere University Press.
Sillanpää, P. (2021). Järjestelmän tietoturvan ja tietosuojan seurannan kehittäminen. Opinnäytetyö, Haaga-Helia-ammattikorkeakoulu.
Sinervo, L.-M., Meklin P. & Vakkuri J. (2015). Oikeudenmukainen kuntatalous. Teoksessa I. Karppi (toim.), Governance – Hallinnan uusia ulottuvuuksia, 97–106. Tampereen yliopisto.
Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31–41.
Siponen, M. & Baskerville, R. L. (2018). Intervention effect rates as a path to research relevance: Information systems security example. Journal of the Association for Information Systems, 19(4), 247–265.
Siponen, M., Klaavuniemi, T. (2021). Demystifying beliefs about the natural sciences in information system. Journal of Information Technology 36(1), 56–68.
Siponen, M.T & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.
Soininen, J. (2001). Henkilöstön hyvinvointi ja työyhteisön murros: Tapaustutkimus Pohjois-Savon ammatillisen koulutuksen kuntayhtymästä. Väitöskirja, Kuopion yliopisto. Pohjois-Savon ammatillisen koulutuksen kuntayhtymä.
Soininen, J. (2021). Tapaustutkimus – toimintamalli IT-johtamisen yhteydestä koulutusorganisaation tuloksellisuuteen koulutuksen reformissa. Väitöskirja, Jyväskylän yliopisto.
Sotto, L. J., Treacy, B. C. & McLellan, M. L. (2010). Privacy and data security risks in cloud computing. World Communications Regulation Report, 5(2), 38.
Sowmiya, B., Abhijith, V. S., Sudersan, S., Sakthi Jaya Sundar, R., Thangavel, M. & Varalakshmi, P. (2021). A survey on security and privacy issues in contact tracing application of Covid-19. SN Computer Science, 2, 136.
Stenberg, M. (2012). Tiedon jakaminen organisaatiossa – kuinka aineetonta pääomaa kasvatetaan. Väitöskirja, Tampereen yliopisto.
Stenbäck, M. (2020). Tietoturvan näkökulma vaatimusmäärittelyssä ja järjestelmäsuunnittelussa. Opinnäytetyö, Tampereen ammattikorkeakoulu.

Stewart, D. & Waddell, D. (2008). Knowledge management: The fundamental component for delivery of quality. Total Quality Management, 19(9), 987–996.
Ståhle, P. & Sotarauta, M. (2002). Alueellisen innovaatiotoiminnan tila, merkitykset ja kehityshaasteet: Esiselvitys. Eduskunnan kanslian julkaisu 8/2002. Tulevaisuusvaliokunta.
Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications, 160, 102642
Sund, R., Nylander, O. & Palonen, T. (2004). Raa'asta rekisteriaineistosta terveyspoliittisesti relevanttiin informaatioon. Yhteiskuntapolitiikka 69(4), 372–379.
Suomela, R. (2016). Hiljainen tieto näkyväksi. Opinnäytetyö, Tampereen ammattikorkeakoulu.
Suonio S. (2023). Pilveen fiksusti – Crayon mukana Cirruksen PIPO-hankkeessa. Blogikirjoitus. https://www.crayon.com/fi/ajankohtaista/blogit/pilveen-fiksusti-crayon-mukana.
Syed-Ikhsan, S. O. S. & Rowland, F. (2004). Benchmarking knowledge management in a public organisation in Malaysia. Benchmarking: An International Journal, 11(3), 238–266.
Syrjänen, P. (2006). Yksityisyyden suoja ja henkilöarviointi. Väitöskirja, Oikeustieteiden laitos, Tampereen yliopisto.
Tabrizchi, H. & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. Journal of Supercomputing, 76(12), 9493–9532.
Taivalmaa, A. (2021). Yksityisyysparadoksi: Systemaattinen kirjallisuuskartoitus. Kandidaatintutkielma, Jyväskylän yliopisto.
Talja, T. (2015). Internet-markkinointi venäläisillä sivustoilla: Yandex & Vkontakte. Opinnäytetyö, Metropolia-ammattikorkeakoulu.
Talus, A., Autio, E., Hänninen, A., Pihamaa, H. T. & Kantonen, S. (2017). Miten valmistautua EU:n tietosuoja-asetukseen? Selvityksiä ja ohjeita 4. Tietosuojavaltuutetun toimisto ja oikeusministeriö.
Telaranta, K. (2017). Enemmän turvallisuutta, vähemmän yksityisyyttä? Politiikasta – ajankohtainen ja ajaton tiedeverkkolehti. https://politiikasta.fi/enemman-turvallisuutta-vahemman-yksityisyytta/
Tietosuojavaltuutetun toimisto (2017). Miten valmistautua EU:n tietosuoja-asetukseen. Haettu 15.7.2019. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf.
Toelle, E. (2021). An introduction to compliance in Microsoft 365. In Microsoft 365 Compliance: A Practical Guide to Managing Risk, pp. 1–31. Apress, Berkeley, CA.

Tuovinen, O. (2015). Varusmiesten johtajakoulutusohjelman kirjallinen oppimateriaali normatiivisen etiikan näkökulmasta. Kandidaatintutkielma, Maanpuolustuskorkeakoulu.
Tähtinen, J. & Kaljonen, A. (1996). Tilastollisen analyysin perusteita kasvatustieteellisessä tutkimuksessa. Turun opettajankoulutuslaitos.
United Nations (2019). Notes on the main issues of cloud computing contracts (prepared by the secretariat of the United Nations Commission on International Trade Law, 2019). Haettu 10.8.2022. https://uncitral.un.org/en/cloud/pre-contract
Vaara, H. (2019). Tietojohtaminen organisaatiokyvykkyyksien kehittämisessä: Tarina perinteisen toimialan organisaatiosta digitalisaatiossa. Opinnäytetyö, Lapin yliopisto.
Valajärvi, J. (2020). Oikeus henkilötietojen poistamiseen ja virheellisen tiedon korjaamiseen: EU:n yleisen tietosuoja-asetuksen tuomat muutokset. Opinnäytetyö, Laurea-ammattikorkea.
Valtiovarainministeriö (2016). EU-tietosuojan kokonaisuudistus. VAHTI-raportti 1/2016.
Valtiovarainministeriö (2022). Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö. Valtiovarainministeriön julkaisuja 2022:43. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164183/VM_2022_43.pdf?sequence=5&isAllowed=y.
Valtiovarainministeriö (2023). Valtionhallinnon pilvipalvelulinjauksien päivittäminen. Lausuntopyyntö, VN/3115/2023.
Van den Berg (2019). Strategic vendor management in co-operation with the European data protection supervisor. The Hague Forum for Cloud Contracting, April 2019.
Veal, A. J. (1997). Research methods for leisure and tourism: A practical guide. 2nd ed., ILAM.
Vilkka, H. (2007). Tutki ja mittaa: Määrällisen tutkimuksen perusteet. Tammi.
Virtanen, P., Stenvall, J., & Rannisto, P.-H. (2015). Julkiseen politiikkaan liittyvä oppiminen ja tietoon perustuva päätöksenteko. Teoksessa Tiedolla johtaminen hallinnossa: Teoriaa ja käytäntöjä, 9–26. Tampere University Press.
Vuorela, M. (2013). Tietämyksen jakaminen kollektiivisesti: Case yritys CGI Suomi Oy. Opinnäytetyö, Turun ammattikorkeakoulu.
Wachter, S. & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 2019(2).
Walliman, N. (2005). Your research project. Sage Publications.
Wang, S. & Noe R. (2010). Knowledge sharing: A review and directions for future research. Human Resource Management Review, 20(2), 115–131. http://doi.org/10.1016/j.hrmr.2009.10.001

Wang, Z., Wang, N., Su, X. & Ge, S. (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. International Journal of Information Management, 50, 387–394.
Wickramasinghe, N. & Bali, R. K. (2008). Knowledge management: The key to network-centric healthcare. International Journal of Biomedical Engineering and Technology, 1(3), 342–352.
Wickramasinghe, N., Bali, R. K., Lehaney, B., Schaffer, J., & Gibbons, M. C. (2009). Healthcare knowledge management primer. Routledge.
Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723–131740.
Yin, R. K. (1983). Case study research: Design and methods. Journal of Management & Organization 22(5), 583–598.
Zhao, H., Jiang, N., Cai, Z., Lim, E. T., & Tan, C. W. (2023). Toward a taxonomy of corporate data protection malpractices and their causal mechanisms: A regulatory view. Journal of Information Technology, 38(3), https://doi.org/10.1177/02683962231155937.

LIITE 1. TUTKIMUKSESSA KÄYTETYT TAUSTAMUUTTUJAT JA VÄITTÄMÄT

Hyvä Vastaanottaja

Suoritan jatko-opintojani Jyväskylän Yliopiston Tietojenkäsittelytieteen laitokselle, tutkimusaiheenani on tiedolla johtaminen tietosuosuojatyössä käytettäessä kansainvälisiä pilvipalveluja. Luotettavan tutkimustuloksen saamiseksi toivon, että vastaat tähän kyselyyn. Lomakkeen täyttämiseen menee aikaa noin 20 minuuttia.

Tiedot käsitellään anonyymisti. Kerätty data käsitellään, arkistoidaan ja tuhotaan olemassa olevien hyvien tutkimusohjeiden ja käytänteiden mukaisesti. Väittämiä on yhtensä 59 kpl, jotka on jaettu kuudelle eri välilehdelle. Niiden alla on Likert-asteikkoon perustuva liukuasteikko. Jokaisen väittämän rinnalla kysytään väittämän merkityksellisyyttä omassa päätöksenteossasi. Valitse myös mielestäsi relevantein vaihtoehto.

Likert-asteikkoon perustuva liukuasteikko: 1= olen täysin eri mieltä, 2= olen eri mieltä, 3= en ole samaa enkä eri mieltä, 4= olen samaa mieltä ja 5 = olen täysin samaa mieltä.

Liu'uta hiiren kursoria (osoitin) kohtaan, joka kuvaa parhaiten mielipidettäsi liittyen esitettyyn väittämään.

Lisäksi lomakkeessa arvioidaan väittämään merkityksellisyyttä omassa päätöksenteossasi. Esitetyn väittämän jälkeen annetaan tälle kolme vaihtoehtoa 1) Merkityksetön, 2) Ei mielipidettä ja 3) Merkityksellinen

Lomakkeen lopussa on ’lähetä’ painike. Klikkaa sitä, kun olet täyttänyt lomakkeen. Huomaa, ettei lomaketta voi lähettää ennen kuin kaikkiin kysymyksiin on vastattu. Voit myös tallentaa osittain täytetyn lomakkeen painamalla ’tallenna keskeneräisenä’ painiketta ja palata vastaamaan myöhemmin. Kun olet täyttänyt lomakkeen kokonaan, muista lähettää se.

Ystävällisin terveisin,

Aapo Immonen.

1 Taustatiedot.

Tämä osio sisältää 9 kysymystä.

1.1 Taustatiedot

Tämä osio sisältää 9 kysymystä.

1.1.1 Koulutusalasi?	[ ] Kasvatustieteellinen koulutusala [ ] Oikeustieteellinen koulutusala [ ] Humanistinen koulutusala [ ] Kaupallinen koulutusala [ ] Luonnontieteellinen koulutusala [ ] Tekninen koulutusala [ ] Maa- ja metsätalousalan koulutusala [ ] Terveys ja -sosiaalialan koulutusala [ ] Palvelualojen koulutusala [ ] Muu koulutusala

1.1.2 Koulutustasosi?	[ ] Erikoisammattikoulutusaste [ ] Alin korkea-aste [ ] Alempi korkeakouluaste [ ] Ylempi korkeakouluaste [ ] Tutkijakoulutusaste [ ] Muu koulutusaste

1.1.3 Valitse esimiestaso, johon kuulut.	[ ] Lähijohtotaso [ ] Keskijohtotaso [ ] Strateginen johtotaso

1.1.4 Kuinka monta vuotta olet toiminut esimiesasemassa?	[ ] Alle 5 vuotta [ ] 5-9 vuotta [ ] 10-14 vuotta [ ] Yli 14 vuotta

1.1.5 Missä Valtorin toimintayksikössä työskentelet?	[ ] Sisäiset palvelut ja viestintä [ ] Tuotanto [ ] Käyttäjätuki [ ] Palvelut ja kehitys [ ] Asiakkuudet [ ] Johto

1.1.6 Millä toimipaikalla työskentelet?	

1.1.7 Kummassa yksikössä työskentelet?	[ ] TORI [ ] TUVE [ ] Molemmissa

1.1.8 Kuinka usein käsittelet työssäsi tietosuojaan liittyviä kysymyksiä?	[ ] Päivittäin [ ] Viisi kertaa viikossa tai harvemmin [ ] Viisi kertaa kahdessa viikossa tai harvemmin [ ] Viisi kertaa kuukaudessa tai harvemmin [ ] En käsittele henkilötiedon käsittelyyn liittyviä kysymyksiä työssäni lainkaan [ ] Ei mikään edellä mainituista

1.1.9 Tietosuojaosaamisesi?	[ ] Erinomainen [ ] Hyvä [ ] Tyydyttävä [ ] Välttävä

2 Hallinnollinen tietosuojatyö.

Tämä osio sisältää 10 kysymystä.

2.1 Hallinnollinen tietosuojatyö.

Tämä osio sisältää 10 kysymystä.

2.1.1 Saan riittävästi informaatiota tietosuojaan liittyvien päätösten tueksi.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.1 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.3 Valtorin ylimmällä johdolla on kokonaisvastuu vaatimusten mukaisen tietosuojan toteuttamiseksi.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.3 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.5 Tietosuojavastaavan toimenkuva on tuotu selkeästi esille Valtorissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.5 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.7 Minulla on riittävästi informaatiota henkilötietojen käsittelyyn liittyvien sopimusten tekemistä varten.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.7 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.9 Olen saanut tarpeeksi informaatiota Privacy Shield järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyssä.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.9 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.11 Olen saanut tarpeeksi informaatiota EU:n mallisopimuslausekkeiden hyödyntämisestä.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.11 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.13 Ennen pilvipalveluiden käyttöönottoa voin hyödyntää näyttöön perustuvaa tietoa arvioidakseni, siirtyvätkö pilvipalveluihin kerätyt henkilötiedot EU alueen ulkopuolelle.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä

2.1.13 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.15 Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa käsiteltävien erityisten (arkaluonteiset) henkilötietojen käsittelyn vaatimustenmukaisuuden.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.15 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.17 Valtorissa järjestetään riittävästi tietosuojakoulutusta.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.17 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

2.1.19 Koulutus tuottaa riittävästi ja tarpeellista informaatiota tietosuojaan liittyen.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
2.1.19 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

3 Operatiivinen tietosuojatyö.

Tämä osio sisältää 9 kysymystä.

3.1 Operatiivinen tietosuojatyö.

Tämä osio sisältää 9 kysymystä.

3.1.1 Tunnistan eri toimijoiden tietosuojaroolit, vastuut ja velvoitteet pilvipalveluissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.1 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

3.1.3 Tunnistan milloin Valtori on rekisterinpitäjä ja milloin se on tietojenkäsittelijä pilvipalveluissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.3 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

3.1.5 Tiedän rekisterinpitäjän ja tietojenkäsittelijöiden vastuut pilvipalveluissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.5 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

3.1.7 Asiakkaille on selvä, milloin he ovat rekisterinpitäjiä käytettäessä pilvipalveluita.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.7 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

3.1.9 Valtorin toimittajat tunnistavat oman roolinsa tietojenkäsittelyssä käytettäessä pilvipalveluita.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.9 Asian merkityksellisyys päätöksenteossa.	[ ] Merkityksetön [ ] Ei mielipidettä

	[ ] Merkityksellinen

3.1.11 Toimijat ovat samaa mieltä rooleistaan, vastuistaan ja velvoitteistaan käsiteltäessä henkilötietoja pilvipalveluissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.11 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

3.1.13 Hyödynnän Valtorin tietosuojaryhmän resursseja tietosuojatyössä.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.13 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

3.1.15 Tietoturvan ja -suojan vuosikelloa hyödynnetään osana pilvipalveluiden turvallisuuden todentamista.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.15 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

3.1.17 Vuosikellon tuottama data antaa informaatiota tietosuojapoikkeamien hallintaan.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
3.1.17 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

4 Tietosuojariskienhallinta.

Tämä osio sisältää 5 kysymystä.

4.1 Tietosuojariskienhallinta.

Tämä osio sisältää 5 kysymystä.

4.1.1 Tietosuojan vaikutusten arviointi on minulle käsitteenä tuttu.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
4.1.1 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

4.1.3 Saan riittävästi informaatiota tietosuojan jäännösriskien arviointia varten ennen pilvipalvelun käyttöönottoa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
4.1.3 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

4.1.5 Valtorissa tunnistetaan jäännösriskit ennen pilvipalveluiden käyttöönottoa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
4.1.5 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

4.1.7 Valtorissa on henkilötietojen käsittely dokumentoitu.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
4.1.7 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

4.1.9 Valtorissa on henkilötietojen käsittely kuvattuna tietovirta kaaviona.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4

	[ ] 5 Täysin samaa mieltä
4.1.9 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5 Tietosuojan ja tietoturvan välinen vuorovaikutus.

Tämä osio sisältää 11 kysymystä.

5.1 Tietosuojan ja tietoturvan välinen vuorovaikutus.

Tämä osio sisältää 11 kysymystä.

5.1.1 Saan riittävästi informaatiota pilvipalveluiden kriisinkestävyyden arviointia varten tietosuojan viitekehyksestä.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.1 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.3 Saan riittävästi informaatiota pilvipalveluiden pääsynhallintaan liittyvien kysymysten arviointia varten tietosuojan viitekehyksestä.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.3 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.5 Saan riittävästi informaatiota, jotta voin arvioida, miten turvallista pilvipalveluissa tapahtuvan henkilötietojen käsittely on. Väittämässä viitataan henkilötietojen siirtoon eri maantieteellisten alueiden välillä.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.5 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.7 Saan riittävästi informaatiota, jotta kykenen arvioimaan	[ ] 1 Täysin eri mieltä [ ] 2

pilvipalveluissa tapahtuvan henkilötietojen säilytyksen vaatimustenmukaisuuden.	[ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.7 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.9 Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluiden varmuuskopioiden ja lokien vaatimustenmukaisuuden.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.9 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.11 Tiedän erityisten (arkaluonteisten) henkilötietojen käsittelyprosessit.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.11 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.13 Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluiden tapahtuvan henkilötietojen pseudonymisoinnin tarpeen.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.13 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.15 Kykenen toimimaan pilvipalveluiden henkilötietojen käsittelyn poikkeamatilanteissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.15 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.17 Tunnen Valtorin henkilötietojen luovutusten prosessin.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.17 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.19 Kykenen toimiman, mikäli pilvipalveluissa ilmenee tietosuojaloukkaus tai sen uhka.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.19 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

5.1.21 Valtorissa on tietosuojaan liittyvä ylläpito- ja kehitystyö vaatimustenmukaista.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
5.1.21 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6 Sisäänrakennettu ja oletusarvoinen tietosuoja

Tämä osio sisältää 15 kysymystä.

6.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

Tämä osio sisältää 15 kysymystä.

6.1.1 Saan tarpeeksi informaatiota tarkoituksenmukaisen henkilötiedonkäsittelyn määrittelemiseksi pilvipalveluissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.1 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.3 Valtorissa käsitellään henkilötietoja tarkoituksenmukaisesti pilvipalveluissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.3 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.5 Saan tarpeeksi informaatiota minimitiedonkäsittelyn vaatimusten määrittelyn toteuttamiseksi pilvipalveluissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.5 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.7 Valtorissa henkilötietojenkäsittelyprosesseissa toteutuu tiedon minimikäsittelyn vaatimukset.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.7 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.9 Valtorissa henkilötietojenkäsittelyprosesseissa on huomioitu tiedon elinkaaren hallinta.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.9 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.11 Käytettäessä pilvipalveluita osoitetaan Valtorissa näyttöön perusten, että henkilötietojen minimikäsittelyn vaatimukset toteutuvat.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.11 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä

	[ ] Merkityksellinen

6.1.13 Valtorissa tietosuojatyö on proaktiivista.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.13 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.15 Valtorissa tunnistetaan tietosuojaan liittyvät riskit ennaltaehkäisevästi.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.15 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.17 Valtori huomioi kaikissa tarjoamissaan pilvipalveluissa henkilötietojen käsittelyssä rekisteröidyn oikeudet.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.17 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.19 Valtorin tarjoamissa pilvipalveluissa on henkilötietojen käsittely läpinäkyvää ja avointa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.19 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.21 Tietosuojatyössä tuotettu informaatio on työssäni päätöksentekoa varten merkityksellistä.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä

6.1.21 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.23 Kykenen tunnistamaan potentiaalisia tietosuojapoikkeamia saadun informaation perusteella.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.23 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.25 Kykenen ennaltaehkäisemään tietosuojapoikkeamia saadun informaation perusteella.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.25 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.27 Tiedän keneltä kysyä tietosuojaan liittyvää informaatiota Valtorissa.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.27 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

6.1.29 Saan tarvitsemani informaation päätöstentekoa varten tietosuojan viitekehyksestä.	[ ] 1 Täysin eri mieltä [ ] 2 [ ] 3 [ ] 4 [ ] 5 Täysin samaa mieltä
6.1.29 Asian merkityksellisyys omassa päätöksenteossani.	[ ] Merkityksetön [ ] Ei mielipidettä [ ] Merkityksellinen

LIITE 2. VÄITTÄMIEN MERKITYKSELLISYYS

TAULUKKO 7. Hallinnollisen tietosuojan osa-alueen väittämien merkityksellisyys

Väittämä	Merkityksetön	Ei mielipidettä	Merkityksellinen
Tunnistan eri toimijoiden tietosuojaroolit, vastuut ja velvoitteet pilvipalveluissa.	2	13	31
Saan riittävästi informaatiota tietosuoajan liittyvien päätösten tueksi.	0	3	43
Valtorin ylimmällä johdolla on kokonaisvastuu vaatimustenmukaisen tietosuojan toteuttamiseksi.	1	10	35
Tietosuojavastaavan toimenkuva on tuotu selkeästi esille Valtorissa.			
Minulla on riittävästi informaatiota henkilötietojen käsittelyyn liittyvien sopimusten tekemistä varten.	5	9	32
Olen saanut tapeiksi informaatiota Privacy Shield järjestelyn mitätöimisen vaikutuksista henkilötietojen käsittelyssä.	5	21	20
Olen saanut tarpeeksi informaatiota EU:n mallisopimuslausekkeiden hyödyntämisestä.	12	22	12
Ennen pilvipalveluiden käyttöönottoa voin hyödyntää näyttöön perustuvaa tietoa arvioidakseni, siirtyvätkö henkilötiedot EU alueen ulkopuolelle.	7	22	12
Saan riittävästi informaatiota, jotta kykenen arvioimaan pilvipalveluissa käsiteltävien erityisten (arkaluotoisten) henkilötietojen käsittelyn vaatimustenmukaisuuden.	5	18	23
Valtorissa järjestetään riittävästi tietosuojakoulutusta.	2	10	34
Koulutus tuottaa riittävästi ja tarpeellista informaatiota tietosuojaan liittyen.	2	11	33

TAULUKKO 8. Operatiivisen tietosuojan osa-alueen väittämien merkityksellisyys

Väittämä	**Merkityksetön**	**Ei mielipidettä**	**Merkityksellinen**
Tunnistan milloin Valtori on rekisterinpitäjä ja milloin se on tietojenkäsittelijä käytettäessä pilvipalveluita.	3	13	30
Tiedän rekisterinpitäjän ja tietojenkäsittelijöiden vastuut käytettäessä pilvipalveluita.	3	15	28
Asiakkaille on selvää, milloin he ovat rekisterinpitäjiä käytettäessä pilvipalveluita.	3	15	28
Valtorin toimittajat tunnistavat oman roolinsa tietojenkäsittelyssä käytettäessä pilvipalveluita.	3	17	26
Toimittajat Valtorin kanssa ovat samaa mieltä rooleistaan, vastuitaan ja velvoitteistaan käytettäessä pilvipalveluita.	3	18	25
Hyödynnän Valtorin tietosuojaresursseja tietosuojatyössä.	2	11	33
Tietosuojan ja -turvan vuosikelloa hyödynnetään osana pilvipalveluiden turvallisuuden todentamista.	2	26	18
Vuosikellon tuottama data antaa informaatiota tietosuojapoikkeamien hallintaan.	**5**	23	18
Tietosuojan vaikutustenarviointi on minulle käsitteenä tuttu.	3	13	30
Valtorissa tunnistetaan tietosuojan jäännösriskit ennen palveluiden käyttöönottoa.	3	17	26

TAULUKKO 9. Tietosuojan riskienhallinnan osa-alueen väittämien merkityksellisyys

Väittämä	**Merkityksetön**	**Ei mielipidettä**	**Merkityksellinen**
Tietosuojan vaikutustenarviointi on minulle käsitteenä tuttu.	3	13	30
Saan riittävästi informaatioita tietosuojan jäännösriskien arviointia varten ennen pilvipalvelun käyttöönottoa.	6	16	24
Valtorissa tunnistetaan jäännösriskit ennen pilvipalveluiden käyttöönottoa.	3	17	26
Valtorissa on henkilötietojen käsittely kuvattuna henkilötietovirtakuvauksina.	3	28	15
Valtorissa henkilötietojenkäsittely on dokumentoitu.	1	10	35

TAULUKKO 10. Tietosuojan ja tietoturvan välisen vuorovaikutuksen osa-alueen väittämien merkityksellisyys

Väittämä	Merkityksetön	Ei mielipidettä	Merkityksellinen
Saan riittävästi informaatiota pilvipalveluiden kriisinkestävyyden arviointia varten tietosuojan viitekehyksestä.	6	23	17
Saan riittävästi informaatioita pilvipalveluiden pääsynhallintaan liittyvien kysymysten arviointia varten tietosuoja viitekehyksestä.	22	27	17
Saan riittävästi informaatioita, jotta voin arvioida, miten turvallista pilvipalveluissa tapahtuva henkilötietojen käsittely on.	3	18	25
Saan riittävästi informaatioita, jotta kykenen arvioiman pilvipalveluiden varmuuskopioiden ja lokienhallinnan vaatimustenmukaisuuden.	5	25	16
Tiedän erityisten (arkaluoteisten) henkilötietojen käsittelyprosessin.	2	8	36
Saan riittävästi informaatioita, jotta kykenen arvioimaan henkilötietojen pseudonymisoinnin tarpeen.	7	22	17
Kykenen toimimaan pilvipalveluissa tapatuvissa henkilötietojen poikkeamatilanteissa.	3	20	23
tunnen Valtorin henkilötietojen luovutusprosessin.	4	13	29
Kykenen toimimaan, mikäli pilvipalveluissa ilmenee tietosuojaan liittyvä poikkeama tai sen uhka.	3	10	33
Valtorissa on tietosuojaan liittyvä tutkimus- ja kehitystyö vaatimustenukaista.	1	14	30

TAULUKKO 11. Oletusarvoisen ja sisäänrakennetun tietosuojan osa-alueen väittämien merkityksellisyys

Väittämä	**Merkityksetön**	**Ei mielipidettä**	**Merkityksellinen**
Saan tarpeeksi informaatiota tarkoituksenmukaisen henkilötietojenkäsittelyn määrittelemiseksi pilvipalveluissa.	4	21	21
Valtorissa käsitellään henkilötietoja tarkoituksenmukaisesti pilvipalveluissa.	4	17	25
Saan tarpeeksi informaatiota tiedon minimikäsittelyvaatimusten määrittelyn toteuttamiseksi pilvipalveluissa.	6	24	16
Valtorissa toteutuu tiedon minimikäsittelyn periaatteet.	2	18	26
Valtorissa toteutuu tiedonelinkaarenhallinnan periaatteet.	2	17	27
Valtorissa tietosuojatyö on proaktiivista.	1	15	30
Kykenen ennaltaehkäisemään tietosuojapoikkeamia.	2	7	27
Saan tarvitsemaani informaation tietosuojan viitekehyksestä.	0	12	34